Dell's storage chronicle

Dell this week is expected to lay out its storage and server road maps. Praveen Asthana, director of Dell storage, talks about the company's storage strategy. **PAGE 10.**

Praveen Asthana

Accelerating Cisco

Cisco has rolled out a suite of products aimed at boosting application performance over the WAN. **PAGE 20.**

The result of endpoint security

Endpoint security checking cannot address all the problems VPN-connected PCs might cause. No matter what the vendors say. **PAGE 30.**

NETWORKWORLD

The leader in network knowledge ■ www.networkworld.com

September 11, 2006 ■ Volume 23, Number 35

Ⓐ WiderNet

Techies under oath

What it's like to be a computer forensics specialist.

BY ANN BEDNARZ

COLIN JOHNSON

During his law enforcement days Harry Megerian got his hands on a lot of IT gear — by brute force.

"We probably did a raid once a week or once every two weeks," says Megerian, a former computer forensics specialist with the U.S. Treasury Department. "I would walk away with five computers, on average."

These days Megerian still scours computers for evidence, but he does it on a consultative basis through the firm he founded, Computer Investigative Services, in Rochester Hills, Mich. One

See Oath, page 76

Momentum building for identity management

BY JOHN FONTANA

Identity management technologies are beginning to weave together the application and network layers of corporate networks, significantly improving access control, easing management burdens and helping users meet stringent compliance and security mandates.

The tools of this emerging trend will be on display this week at the annual Digital ID World conference in Santa Clara, where vendors such as Apere, Applied Identity, Caymas, ConSentry Networks, Identity Engines and Trusted Network Technologies (TNT) will display their network access control (NAC) gear. NAC relies on identity to determine which machines get on the network — and more important, what users are authorized to do once there.

While NAC is gaining momentum, users and analysts say the unification of the network and application layers via identity is a missing link to reducing risk in a compliance-driven world where access is expected from anywhere and network perimeters are disappearing.

"It is becoming more important to know who is on the other end of the wire," says Jon Oltsik, senior analyst for information security at the Enterprise Strategy Group. "Security, compliance and global business initiatives are going to drive these two [layers] together."

To underscore this emergence of sophisticated NAC options, Cisco and Microsoft last week at the Security Standard conference introduced a white paper detailing how users can integrate Cisco's Network Admission Control and Microsoft's Network Access Protection (NAP) technologies. The companies said they would support each other's protocols, but stuck to their previous statements that they would

See Identity, page 74

Managing risk: new reality for IT security executives

BY DENISE DUBIE

THE SECURITY STANDARD

BOSTON — Security executives from around the country converged on Boston last week to hear how their peers are tackling enterprise security and managing risk.

The Security Standard conference, hosted by *Network World* and other IDG publications, examined such issues as regulatory compliance, dealing with internal and external threats, working with law enforcement and establishing

See Security, page 14

CLEAR CHOICE TEST

Intrusion-prevention systems

You want your IPS to block all exploits and to move traffic at multigigabit rates.

We tested top-of-the-line IPSs and found the products force a tradeoff between screaming performance and airtight security.

Page 38.

VON show takes aim at branch office set

BY PHIL HOCHMUTH

The Voice on the Net show is set to open in Boston this week, featuring VoIP products and services aimed at helping smaller companies, or those with branch offices, set up and manage packetized voice traffic.

In its ninth year, VON is expected to draw about 300 exhibitors, 330 speakers and an estimated 8,000 attendees. The show will take place in the midst of a torrent of growth in almost all sectors of the VoIP industry, from business and consumer VoIP services to enterprise and carrier gear, industry analysts say. Statistics from Telegeography Research and Dell'Oro Group indicate the magnitude of this growth:

- 6.9 million VoIP subscribers added in the second quarter of 2006.
- $607 million in VoIP services revenue in the second quarter of 2006, an almost 200% increase from the second quarter of 2005.

See VON, page 16

IBM

INNOVATIONS IN access

Florida Guardian ad Litem **Saw the Future** of Child Advocacy.

Citrix Provided Access.

"Custody rulings. Foster care. Adoptions. Our founding vision was to give every abused and neglected child in Florida a strong advocate in court. Two years later, we're well on our way. Today, program staff, attorneys and over 5,000 volunteers represent more than 27,000 children. Instead of information in file drawers scattered all over the state, Citrix software gives advocates secure access to our case management system from anywhere. Resources are precious, so we must apply them wisely, not waste time chasing data. These kids depend on us. That's why we're depending on Citrix to take us the rest of the way to advocate for every Florida child in need."

JOHNNY C. WHITE
CIO
Florida Guardian ad Litem Program

Access your future today at citrix.com.

CITRIX®

NETWORKWORLD

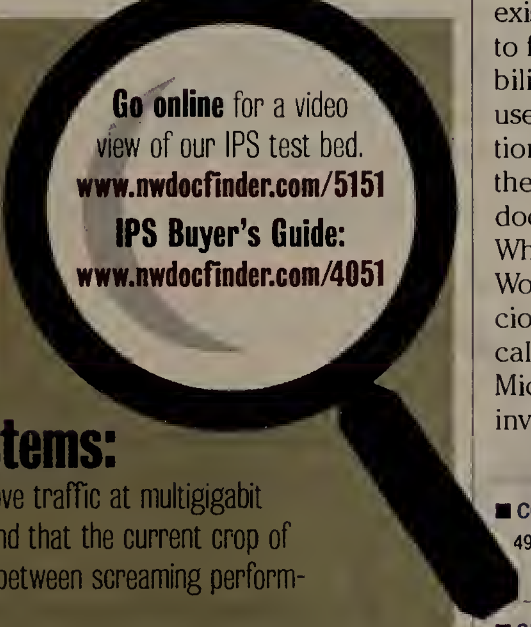
9.11.06

COOLTOOLS

Show your colors with a 1GB USB drive with a preseason top 25 college football logo. Page 34.

Features

NETWORKWORLD CLEAR CHOICE



Go online for a video view of our IPS test bed. **www.nwdocfinder.com/5151**

IPS Buyer's Guide: www.nwdocfinder.com/4051

Intrusion-prevention systems:

You want your IPS to block all exploits and to move traffic at multigigabit rates. We tested six top-of-the-line IPSs and found that the current crop of products forces customers to make a trade-off between screaming performance and airtight security. **Page 38.**

Newsbits

Microsoft cuts you a patch break

■ After handling 19 sets of patches in July and August, system administrators will catch a bit of a break next week when Microsoft is expected to release three security updates for its Windows and Office products. Last week the software giant said that only one of these updates — for Office — is rated critical. The updates will be released Tuesday in line with Microsoft's monthly patch release schedule. The other two updates, which fix problems with Windows, are rated no higher than important, meaning that user action is required before an attack based on these flaws could succeed. Microsoft did not release any further details on the patches. The company's advance notification on the updates can be found at www.nwdocfinder.com/5176.

Meanwhile, Windows flaw causing problems

■ Microsoft may or may not be patching a flaw Symantec last week warned users about. An unpatched fault in the Windows 2000 version of Microsoft Office 2000 is being used by attackers to run unauthorized software on a victim's computer, the security company said. Microsoft confirmed that the bug exists, but would not say when it plans to fix the problem. The critical vulnerability was first reported by Symantec to users of its DeepSight threat notification service. Attackers are exploiting the flaw by sending malicious Word documents to victims, Symantec said. When these documents are opened, Word is tricked into installing malicious software on the PC. Symantec is calling this malware Trojan.MDropper. Microsoft may issue a patch once its investigation is complete.

NIST wants teamwork on security issues

■ The National Institute of Standards and Technology, which maintains a database of software product vulnerabilities as a public reference, last week invited closer contact with the industry to clarify and resolve disputed vulnerability information. NIST will work more closely with vendors by letting them post information clarifying how vulnerabilities may affect their products, said Peter Mell, senior computer scientist at NIST, the federal agency that manages the National Vulnerability Database. The NVD contains information about 19,200 vulnerabilities identified in software products over the past eight years. NIST aggregates vulnerability data with information that references vendors and their products. Sometimes the impact of a vulnerability is dis-

See Briefs, page 6

■ **CONTACT US** Network World, 118 Turnpike Road, Southborough, MA 01772; **Phone:** (508) 460-3333; **Fax:** (508) 490-6438; **E-mail:** nwnews@nww.com; **STAFF:** See the masthead on page 16 for more contact information. **REPRINTS:** (717) 399-1900

■ **SUBSCRIPTIONS/CHANGE OF ADDRESS: Phone:** (508) 490-6444; **Fax:** (508) 490-6400; **E-mail:** nwcirc@nww.com; **URL:** www.subscribenw.com

Newsbits

Briefs

continued from page 5

puted. While vendors can post their opinions on their own Web sites or elsewhere, until now they weren't included in the NVD.

Qwest racks up deals

■ Qwest Communications is on a roll, racking up several key multimillion-dollar state government contract wins and renewals this year. The victories come at a time when state governments are consolidating networks and pushing carriers to reduce rates. Qwest won't release data about the size of its state government business, but officials confirmed that sales are up this year. Qwest says it is cutting rates to retain state government business in its 14-state region, where it is often the incumbent carrier. In addition to local and long-distance services, Qwest is pursuing bids that involve telecom repair, network equipment integration and 911 services for state agencies. Recent wins for Qwest include a two-year, $20 million deal announced in August to install and maintain Cisco hardware for Minnesota's WAN, and a deal announced in April to provide Internet service to Ohio's public K-12 schools. The dollar value of the Ohio deal was not released. Additionally, the company landed a six-year, $24.7 million agreement in February to provide network services to more than 400 Wyoming public schools.

Mozilla taps ex-Microsoft exec

Window Snyder

■ Mozilla has hired Window Snyder, a former Microsoft security strategist, to help lock down its open source products against online attacks. Snyder has worked on Microsoft's security-driven Windows XP Service Pack 2 update and also had a role in the development of Windows Server 2003. Snyder will take charge of Mozilla's security strategy.

India may use cybercrime court

■ India's National Association of Software and Service Companies has asked the Indian government to set up a special court to try cybercrimes and other offenses under the country's Information Technology Act 2000. Having a special court will ensure that cybercrime trials will be faster than in ordinary Indian courts, NASSCOM says. Indian court cases last an average of about three years. None of the trials of persons charged in India for data fraud has as yet come for conviction and sentencing, NASSCOM says. The request for a special court is part of a multipronged strategy by NASSCOM to strengthen data protection and privacy in India's outsourcing industry. NASSCOM's initiatives come in the wake of allegations in the United States and the United Kingdom that Indian call-center workers have stolen and sold data processed by Indian outsourcing companies. India's outsourcing industry has a better record in protecting customer data and privacy than the United States, according to NASSCOM.

Bug found in ICQ client

■ AOL is advising users of its ICQ instant-message service to update to the latest version of the IM software following the discovery of a bug in an older version of the product. Security researchers at Core Security last week reported they discovered the flaw in ICQ Pro 2003b, a version of the ICQ client that AOL offers for download. Although the bug doesn't affect more recent ICQ software such as ICQ 5.1, Core researchers have developed proof-of-concept code that causes ICQ Pro 2003b to crash. They believe this vulnerability could be exploited to run unauthorized software on a user's PC. More information on this flaw can be found at www.nwdocfinder.com/5177. AOL said it was working to fix the bugs, but the company classifies them as minor and low-risk.

{quote of the week}

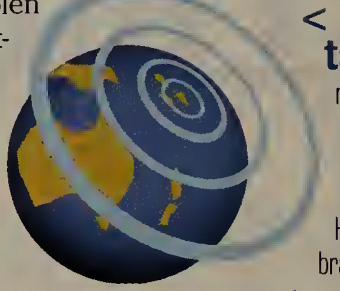
"WLAN is, if not dead, then uninteresting."

Dominic Orr, CEO of Aruba Wireless Networks, discussing his company's focus on more than just wireless network security.

Roadrunner burns up the racks

■ IBM will build a next-generation supercomputer for the U.S. Energy Department that has the potential to achieve a sustained speed of 1,000 trillion calculations per second, or one petaflop. The computer, dubbed Roadrunner, will be built at the Los Alamos National Laboratory in New Mexico. Congress provided $35 million in fiscal 2006, which ends on Sept. 30, to launch the computer project. Roadrunner may eventually be used for an Energy Department program that ensures the U.S. stockpile of nuclear weapons is safe, the Energy Department says. The machine will use commercially available hardware and be based on the Red Hat Linux Version 4.3 operating system. IBM System x3755 systems based on Advanced Micro Devices Opteron technology will be deployed in conjunction with IBM BladeCenter H systems with Cell technology.

TheGoodTheBadTheUgly



< Getting an early read on tsunamis. Governments seeking inexpensive technology to warn of tsunamis could be interested in a free software application that monitors vibrations in the hard disks of computers in an attempt to detect the undersea earthquakes that cause tsunamis. The Tsunami Harddisk Detector (www.ninsight.at/tsunami/) is the brainchild of Michael Stadler, who demonstrated the prototype system in Austria.

SAP gets sued. I2 Technologies accused SAP of patent infringement in a lawsuit filed Tuesday. A maker of supply chain management software, i2 claims that SAP has infringed seven patents granted between 1998 and 2006. The alleged infringements relate to models and tools in areas such as managing factory planning systems, negotiating and tracking the sale of goods, and allocating manufactured products to sellers. SAP is investigating the charges.

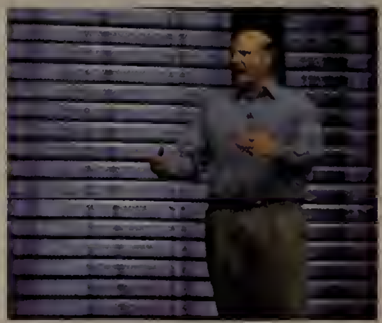
HP board brouhaha revealed. All's not well in the higher echelons of HP, as revealed in a filing the company made to the Securities and Exchange Commission on Wednesday. The controversy relates to the sudden and unexpected resignation of Silicon Valley venture capitalist Thomas Perkins from HP's board of directors in May. According to an 8-K filing HP made to the SEC, he quit over concerns with the board's handling of investigations into leaks of confidential information.

Alleged Web site scheme halted

■ A U.S. district court has ordered a halt to an operation that allegedly added unauthorized charges to the phone bills of small businesses and nonprofit groups for Web-site services that, in many cases, they didn't request or know they had, the U.S. Federal Trade Commission said. The FTC's original complaint named defendants WebSource Media, BizSitePro, Eversites, Telsource Solutions, Telsource International, Marc Smith, Kathleen Smalley, Keith Hendrick, Steven Kennedy, John Ring and James McCubbin Jr. The defendants illegally billed thousands of customers, the FTC says. The operation was a maze of interrelated companies directed by the defendants, the FTC said. It used telemarketers to make cold calls to small businesses and nonprofits and offered a free 15-day trial of a Web site design. The customers were told there was no charge or obligation and the Web site would be cancelled automatically if it was not approved by them. The customers' phone bills were often charged even if they did not agree to be billed after the trial.

Layer 8

"If somebody doesn't get this @&# demo to work, I'm coming over there with a chair!"*



Dale Worley of Elkridge, Md., wins this week's contest. Try your hand each week with our new contest. www.networkworld.com/weblogs/layer8

PEERSAY

From our online forums

■ **Router loopback.** User rrmiles details a problem in letting wireless users log into a Cisco PIX — all that results is loopback from the LAN to the WAN port. Take a look at his configuration and offer suggestions.
www.nwdocfinder.com/5168

■ **What users say about you, part 1.** User Jimbo discusses users: "I'm a manager, not a grunt, and the fact that I'm doing something at your computer means that you probably cornered me in the elevator or on the way from a meeting. You can't be bothered to call for desktop support, and I've got things to do that don't involve desktop support. I've got desktop grunts for that. Call the Helpdesk."
www.nwdocfinder.com/5169

■ **What users say about you, part 2.** User Tantor writes: "Yes, maintaining servers and network infastructure is important, but if the users don't know how to make use of it, what is the good of this technology? Sitting down with staff for 30 minutes to show them how to access e-mail, network shares, shared calendars, intranet pages, etc., simplifies the user's life, and your life because they won't call you wondering how to access something. And if you can't do something for users, then explain why rather then just saying 'no.' People skills are just as important as technical skills."
www.nwdocfinder.com/5170

■ **iPod killers?** User Craig reads a blog post by Cool Tools Editor Keith Shaw on two iPod competitors: "All you have to do is underprice the iPod (which is extremely overpriced) and offer standard formats . . . Apple can keep the iPod and their proprietary formats." See how Shaw replies.
www.nwdocfinder.com/5171

■ **Traffic-shaper coexistence.** User Zort is seeking help for an optimization issue: Has anybody deployed Riverbed Steelhead appliances on a network that already has PacketShaper running on it?
www.nwdocfinder.com/5175

networkworld.com

■ FOLLOW THESE LINKS TO MORE RESOURCES ONLINE

BLOGOSPHERE

Microsoft beats Apple?

Plus: Google's fading luster, Bud TV and typo trouble

Microsoft beats Apple at reviewer relations? Blogger James Gaskin recently discussed small-business servers, but left out Apple. Why? Gaskin says it's because Apple won't send him any products to review, ever. "Apple provides the least help to writers of any major vendor of hardware or software," he writes. Contrast that with Microsoft, which gets Gaskin products overnight. But at least one reader has told him he's just not talking to the right people at Apple.

www.nwdocfinder.com/5152

Slip of the finger. A couple of weeks ago *Network World* published one of our DocFinders in these very pages — only we got the URL wrong. Instead of publishing "www.nwdocfinder.com/4957", we flubbed the domain name — and as Adam Gaffin points out in Compendium, some enterprising cybersquatter jumped on it. (Rest assured, the DocFinder link below is correct.)

www.nwdocfinder.com/5154

Google not omnipotent. Has Google strayed from its strengths? In Gibbsblog, Mark Gibbs adds his two cents to the blogosphere's conversation about how Google is going about its business. With all its new products, which are really good, and which should be dropped? And what has Google done for us lately?

www.nwdocfinder.com/5153

Budweiser to launch Web TV. Layer 8 reports that Budweiser is getting into the Web video business. The goal? To sell beer, of course. But in an entertaining way that involves comedy and of course, reality shows.

www.nwdocfinder.com/5155

ITVIDEO *Hot Seat interviews, the coolest tools, and more*

Hot Seat: Using the mental finger-print. Verid CEO Kevin Watson talks about a new method of using "mental finger-prints" to protect online transactions.
www.nwdocfinder.com/5163

Cool Tools: You can't beat USB. Keith Shaw highlights some of the latest USB flash drives, which include applications such as antispyware scanners. There's even a drive that forces strong passwords and automatic encryption.
www.nwdocfinder.com/5164

Podcasts: *Network World's Twisted Pair:* Jason Meserve and Keith Shaw rant about the HP board of directors soap opera, Intel's job cuts, more gadget recalls and whether people can really have "telephone telepathy."
www.nwdocfinder.com/5165

ASK THE HELPDESK *Find the answers to these prickly problems online.*

■ **This week:** Determining what LAN tools to have in your tool belt.

Ron Nutter helps a user just starting out figure which LAN tools he simply must have.
HelpDesk response:
www.nwdocfinder.com/5172

Andreas M. Antonopolous provides three tips for reducing storage total cost of ownership.
HelpDesk response:
www.nwdocfinder.com/5173

M.E. Kabay explores some of the legal issues surrounding enterprise technology.
HelpDesk response:
www.nwdocfinder.com/5174

Mark Gibbs looks at a tool to make RSS generation easier.
HelpDesk response:
www.nwdocfinder.com/5175

BEST OF NW'S NEWSLETTERS

WAN lessons learned

Plus: How to hide your online footprints.

Wide-area networking: A reader of this newsletter shares the experience of working with a medical clinic that decided to run its medical appointment application over a carrier's frame relay network instead of over the clinic's existing regional T-1 private line. As analysts Steve Taylor and Larry Hettick report, the project illustrates how not to deploy an application over a WAN.
www.nwdocfinder.com/5125

Web applications: Everywhere you browse on the Web you leave traces. Even if you're only mildly paranoid, you might wonder just what can be known about you from these "footprints." To counter this problem, a new free service has been launched: Lost in the Crowd from Unspam Technologies. Columnist Mark Gibbs explains how it works.
www.nwdocfinder.com/5126

Linux: Linux users who applied Ubuntu's most recent software upgrade were given a reminder of the early days of Linux; a flaw in the code rendered the GUIs on the machines useless, forcing users to navigate directories and run programs through — gulp! — the command-line interface of Linux. Senior Editor Phil Hochmuth reports.
www.nwdocfinder.com/5127

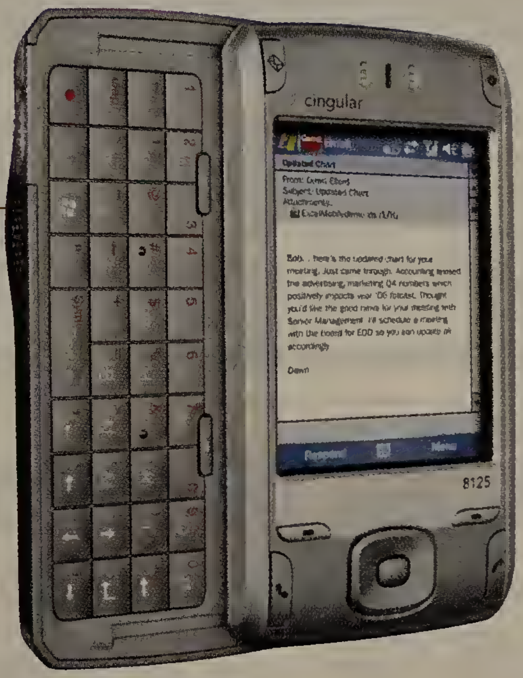
Storage in the enterprise: Analyst Mike Karp writes: "The battle going on right now between Intel and AMD for the hearts of CPU lovers everywhere reflects a similar state in storage.
www.nwdocfinder.com/5128

Free e-mail newsletters
Sign up for any of more than 40 newsletters on key network topics.
www.nwdocfinder.com/1002

Wireless email

now is a business tool, not a perk.

Give your employees the tool to keep them connected even when they're out of the office. Give them Cingular's real-time wireless email and watch productivity skyrocket. Give them now.



CINGULAR 8125

- Solutions are easy to implement and scalable to meet a business's growing needs.
- Triple data encryption ensures critical information stays secure.
- 24/7 customer support for worry-free service.
- From the #1 provider of wireless email for business.
- Runs on ALLOVER,™ the largest digital voice and data network in America.

CINGULAR MAKES BUSINESS RUN BETTER

Call 1-866-4CWS-B2B Click www.cingular.com/wirelessemail Contact your account representative

cingular
raising the bar™

The ALLOVER network covers over 273 million people and is growing. **Coverage** not available in all areas. Certain email systems may require additional hardware and/or software to access.

Q&A Dell exec talks storage strategy

At its annual Technology Day in New York this week, Dell is expected to talk about its storage and server road maps and make what it says is a significant storage announcement. Network World *Senior Editor Deni Connor caught up with Praveen Asthana, director of Dell storage, and talked about the company's storage strategy. Although Asthana discussed where Dell is going in storage, he declined to comment on this week's storage news or the company's rumored OEM relationship with Overland Storage for low-end tape library products, or with Engenio for low-end disk.*

> “[C]ustomers are spending more than 40% of their storage budget on disk already and they have 50% to 100% data growth, but their storage budget isn't growing by much.”

Praveen Asthana, director of Dell Storage

So how do you see the state of the storage market over the next six months for Dell?

We are seeing lots of data growth, lots of complexity and lots of cost. We have government regulations to worry about, customers are spending more than 40% of their storage budget on disk already and they have 50% to 100% data growth, but their storage budget isn't growing by much. Customers need a way to solve this equation.

What common themes do you see in storage?

We are pushing on the basic themes of storage — simplicity, affordability and balanced scalability. If you look at simplicity, one of the trends we are driving is reducing deployment costs and the complexity of storage so storage is as easy to install as servers are right now. There are products from Dell that do that — one of them is the entry-level AX100 storage-area network array.

If you look at affordability, there are key technologies we are pushing hard on such as Serial [Advanced Technology Attachment] drives. We introduced a direct-attached array, the MD1000, earlier this year — it has both Serial Attached SCSI and Serial ATA compatibility. ISCSI is another technology that has been talked about as the technology of the future — we are actually seeing a lot more pickup of it this year. We have the AX150 array that has both iSCSI and Fibre Channel capability. These products are primarily playing to our customer base, which is midsize businesses who are looking for easy-to-use, simple storage.

How do the data needs of those smaller customers differ from those of larger businesses?

We often find that small customers have the same data-storage needs as larger customers, but they don't have the budgets. They are looking for capable storage at entry-level pricing. We are adding more functionality into our storage.

How are you adding that functionality?

We are putting in snapshot capability, mirroring and replication.

You talk of the notion of balanced scalability. What do you mean by that?

If you look at a customer's infrastructure, it will consist of multiple components that scale independently but somehow depend on each other for operation. You can have primary disk storage, secondary storage, tape, management software and servers. What happens as data needs grow is that customers will have to do forklift upgrades because their gear can't be upgraded. That's expensive. We are pushing modularity in everything we sell, so you can do balanced scaling without having to do forklift upgrades. ■

IBM, HP boost client-management wares

BY DENISE DUBIE

IBM and HP last week separately announced updated systems-management software designed to make it easier for customers to deploy programs to client machines and to cut the cost and manual effort needed to maintain desktops.

IBM says its Tivoli Provisioning Manager 5.1 can help IT staff automate parts of the process to deploy and decommission laptops, desktops, wireless devices and servers. The product includes technologies that can gauge when to distribute software to clients based on available network bandwidth. The software can “sense” the utilization of the network using TCP/IP protocols and adapt software distribution accordingly, IBM says.

“This feature enables the product to be aware of how the network is being used for business needs at a given time and help IT staff to reduce resource requirements and avoid overprovisioning to accommodate software distribution,” says Dave Lindquist, IBM Tivoli chief architect. “The updates shouldn't impact network traffic or an end user's experience.”

The software also can reduce the impact of software rollouts on the network with a new peering feature, which lets clients download updates from a local server or desktop if the network traffic or high server volume slows the process. Based on grid technology, the peering capability enables files, such as e-mail applications or video clips, to be downloaded from a nearby system, rather then directly from the central distribution software, to ease the burden on traffic and that server.

“The features such as adaptive bandwidth control and peering are network and systems performance-related upgrades, which is a bit of a different direction for software distribution technology,” says Joe Clabby, president of research firm Clabby Analytics. “IBM is automating workflows and the pragmatic processes within IT shops. The idea of doing software updates en masse without wreaking havoc on performance will hit IT managers where they live.”

This release incorporates technology IBM acquired with Rembo Technologies in June. At that time, IBM said Rembo software performs “the bare metal basic operating system install,” a gap in IBM's offerings. Integrated into Tivoli Provisioning Manager, the Rembo software uses a differencing technology that stores and saves the various customizations in client and server operating systems images to maintain the changes and enable speedier recovery if a system needs to be rebuilt.

The software installs on a dedicated server (ranging from AIX to Windows to Linux to Solaris) and can deploy IT components ranging from virtual servers and middleware to network devices acting as routers or load balancers, IBM says. IT managers also can set up depot servers from which to install packages on targeted client and server machines, depending on the size of the environment and how IT managers would like to distribute software.

Tivoli Provisioning Manager 5.1 costs $1,100 per managed processor and $65 per managed client.

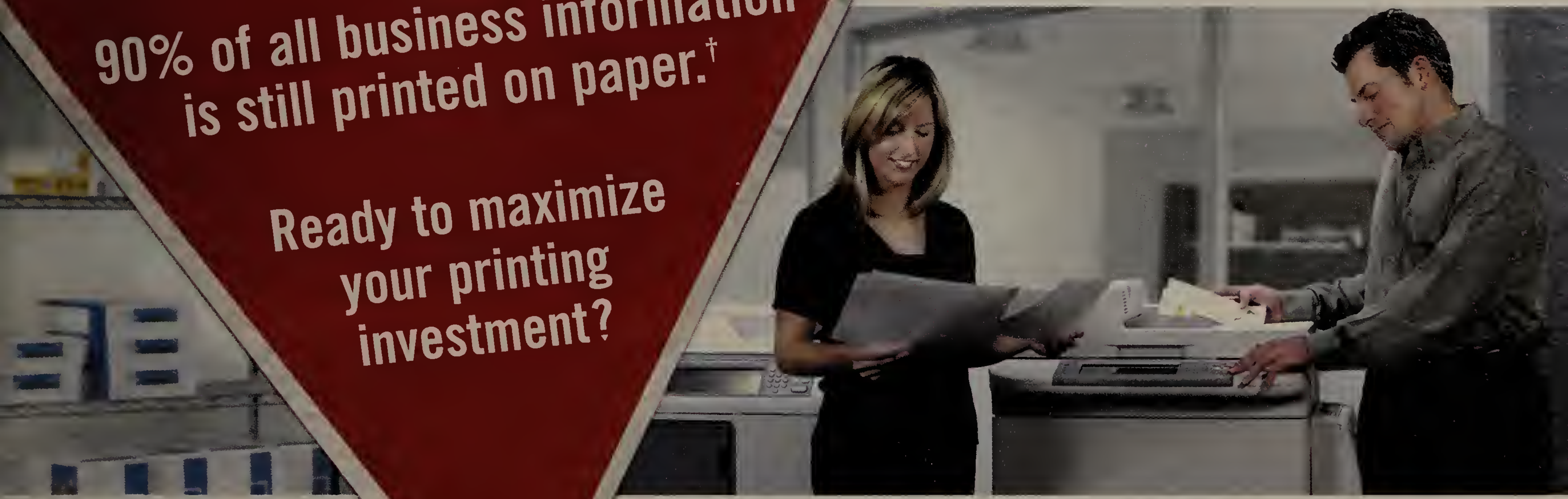
For its part, HP last week announced that OpenView Client Configuration Manager 2.0 includes new features to remotely deploy and migrate operating systems using image technology. This version includes a feature for capturing customized user settings, which HP says makes it easier to port those settings to different PCs and operating systems. The software also has been upgraded to track software use, which could result in license savings.

The company says commercial HP laptops, desktops and workstations will begin shipping with a preloaded HP OpenView Configuration Management agent to help cut costs. The software has been updated to manage assorted vendors' Windows-based clients as well as HP thin clients.

Industry watchers say HP is helping customers by adding features but also by embedding technology onto HP hardware.

“It's important because it adds modules and functions to make it a more complete solution [for customers] and a better product for [HP's Personal Systems Group],” says Ronni Colville, a research vice president with Gartner.

HP OpenView Client Configuration Manager 2.0 is expected to be available next month. Starting price is $75 per seat license. The preloaded HP OpenView Configuration Management agent is shipping now with select HP computers. ■



Brocade expanding SAN software

BY DENI CONNOR

Brocade blooms

A list of some of the product enhancements or new products Brocade is announcing.

Product	What product does	What's new
Application Resource Manager v2.0	Allows SAN-based provisioning of servers.	Automated system failover, support for Fibre Channel and iSCSI.
Brocade Access Gateway for Bladed Servers	Provides access to the Fibre Channel SAN for blade servers.	New, first or second quarter of 2007.
Data Migration Manager v2.0	Migration tool for moving data from one array to another.	Migration capability when systems are offline.
Silkworm FC4-16IP	Eight-port iSCSI blade for Silkworm 48000 Director.	New, available fourth quarter.
Silkworm FC4-48 blade	48-port blade for Silkworm 48000 Director.	New; available fourth quarter.

Brocade Commuications this week is set to announce new versions of its file-aggregation and -access software that it says will let customers tap into and manage data more easily while letting them provision servers on the fly.

Data Migration Manager now can be used to move data when the storage system is online, resulting in migration of data without disruption of operations. Application Resource Manager now has provisions for the automated failover of servers and connection to iSCSI networks. Brocade also has improved StorageX performance and global namespace scalablity and added policies and reports on file replication. The company acquired the software products a year ago from NuView and Therion.

In its traditional Fibre Channel switching line of business, the company will roll out a 48-port Fibre Channel blade and an eight-port iSCSI blade for its Silkworm 48000 Director level switch, which lets users build larger, more scalable multiprotocol storage-area networks (SAN). The company also will introduce an Access Gateway for bladed servers, as well as SAN extension gear that offers interoperability with McData switches, encryption and improved WAN analysis tools.

"On the blades and switches, Brocade is providing full 4Gbps performance and iSCSI support with no port tax, so end users don't need to sacrifice a port to get multiprotocol support or higher performance or density or redundancy," says William Hurley, senior analyst with the Data Mobility Group.

Beset with increasing competition from Cisco for its core business, Brocade this year set out to protect itself from further market-share encroachment from Cisco by buying one of the last remaining Fibre Channel vendors, McData, for $713 million. The purchase aims to reestablish Brocade as the market leader in Fibre Channel director-level switches with two-thirds market share.

According to research from Dell'Oro Group, Cisco edged out Brocade for the first time in the second quarter of 2006 in director-level switches. Cisco had a 33.6% market share, followed by Brocade with 33.3% and McData with 32.9%.

In 2002 Brocade acquired Rhapsody Networks, a maker of Fibre Channel intelligent switches. Its product became the basis for the Brocade Silkworm Fabric Application Platform, which now provides switch-based storage virtualization.

"We are trying to grow our core business — Fibre Channel switching. We are also diversifying our business into adjacent markets, because we believe that shared storage is the model by which enterprises get efficiencies and can better manage their data," says Mario Blandini, director of product marketing for Brocade.

Blandini says Brocade's goal by the end of fiscal year 2006 is to have 5% of its revenue from professional services, 5% from its Tapestry file and SAN provisioning products and 90% from its traditional Fibre Channel gear business. Adding the professional services organization from McData to this mix is expected to increase revenues when the deal closes in the first quarter of 2007.

Brocade has done well with its acquisitions, users and analysts say.

"Enhancements to the NuView storage software shows that Brocade is seriously committed to pushing the technology forward and that robust file sharing is a real problem in all organizations, large and small," Hurley says.

"When you are in acquisition mode there is a certain amount of time it takes to get things to a point where your offering is a lot better than just the individual products," says Leon Verriere, manager of systems engineering for Mohawk Industries in Dallas, which is a Brocade and NuView customer.

"While Brocade has done a good job of integrating products so far, they still have work to do. These acquisitions elevate Brocade to a much higher level," he says.■

CA pumps up Unicenter with automation

Company includes technologies to ease deployment and enhance correlation capabilities.

BY DENISE DUBIE

CA this week is making available a version of its flagship network- and systems-management software that the company says includes features to more quickly identify the root cause of problems and more intelligently monitor networks.

With Unicenter Network and Systems Management (NSM) 11.1, CA delivers on its promise of better integrating existing products and providing customers with a management database, industry watchers say. The company last fall at its annual user conference announced the management database.

"The [management database] feeds information to management tools that administrators use to do their particular jobs, whether it is troubleshooting or compliance reporting or asset management," says Jasmine Noel, a principal analyst with Ptak, Noel & Associates. "It is very important to have the [management database] working well. CA seems to be running a close second to BMC in terms of delivered capabilities."

Customers seem most taken with enhancements to its event-correlation engine, which helps IT managers more quickly find the root cause of performance problems, and added intelligence in its agents. The correlation features are part of CA's Management Command Center, which displays related alerts and problem areas in a dashboard-style view.

The company says intelligence in its software agent technology enables the software to provide baselines for normal events and alerts on managed devices and adjust the monitoring thresholds accordingly. This adaptive configuration capability reduces the amount of false alerts, lessens the need for systems administrators to manually adjust agent configuration and lets IT staff focus on the real problems, CA says.

Cody Lowder says the updated correlation and agent technology are two must-haves he suggested CA include while he beta-tested the software in the past year. The information systems and technology manager of Enterprise Management at Zions Management Services, a collection of banks distributed around the country with more than 1,000 branches, says the upgraded correlation engine includes a better user interface, which pinpoints problems much quicker.

"One of the big problems with monitoring large environments is that it is hard to discover the initial problem that caused all the dominoes to fall," Lowder says. "Right now I send a bunch of notifications to a bunch of people about problems, but this seems like it would help us reduce the noise and notifications we send to technicians."

The upgraded agent technology will make it easier for Lowder and his staff to update distributed agents from a central source without having to log on to the server. But CA still could add the ability to discover and install agents on servers automatically in its software, he says. Lowder adds he has to do the initial install of the agent, but CA has made it easier to update and configure the agents after the initial manual install.

"CA has come a long way, but if I have a new server come online, I have to get the agent started," he says. "It would be nicer to have that automated as well."

The company also integrated software previously available as add-ons into the core offering. The add-on software that is part of NSM 11.1 includes Active Directory Management Option, NSM Systems Performance Option, NSM Monitoring Option for z/OS and Unicenter Management Portal.

Unicenter NSM uses central manager software and distributed-agent technology to collect data from and take action on managed devices. Unicenter NSM 11.1 is priced by separate components. The manager component is $2,000, and each resource being managed is an additional variable cost, starting at $2,200.■

Security

continued from page 1

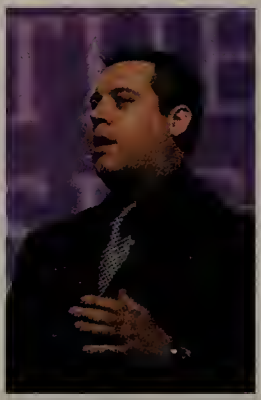
security best practices.

The conference also provided a forum in which security executives could explore how their responsibilities are changing and how they dovetail with more holistic concerns about corporate health.

Speaker Jason Jackson, director of emergency management at Wal-Mart Stores, said, "We should know what a hazard or risk could mean to our businesses, whether it's a natural disaster or man-made attack, before it happens. Having a corporate structure in place regarding crisis is sometimes more important than having a detailed plan on how to react to specific events."

Creating a culture

IT security is focused primarily on protecting the perimeter, but with internal data leaks and security breaches topping the news, security executives today are seeking measures to protect customer data and corporate intellectual property across the organization.



"We should know what a hazard or risk could mean to our businesses — whether it's a natural disaster or manmade attack — before it happens."

Jason Jackson, director of emergency management, Wal-Mart Stores

TRACY POWELL

We are still "hard and crunchy on the outside, but soft and chewy on the inside," said Dixon Greenfield, manager of data center operations at Valmont Industries, a manufacturing company in Valley, Neb. "So I need security at all the layers, but I've got certain sets of data that I'd like to have more secure than others."

Security experts say the trick to building a more security-aware culture is finding the right mix of processes and technology that suit the business, and then educating the IT staff and user community on how to maintain secure practices.

Sean Franklin, an IT security manager at a large financial services firm, said, "People are our weakest links. Most of our wounds are still self-inflicted. Configuration changes that aren't well thought out and leave us open and exposed in certain areas are still the hardest things to lick."

Part of the problem lies in the fact that employees aren't as technology- or security-savvy as the IT staff and often don't realize when their actions — or lack thereof — pose a risk.

"They don't take it as seriously, so getting across the message that little things that have to be implemented and can be irritating is, well, it's a process," Greenfield said.

A first step in creating a security-minded culture is making it clear why certain security policies are in place. It's important to make sure security measures don't impede business processes, industry watchers say, but if need to, the IT security staff must educate users why they have to take such precautions.

"IT managers assume end users know why they can't, for instance, download music files," said Zeus Kerravala, a vice president with Yankee Group. "The end user may think the policy is in place to prevent bandwidth hogging — when really it's to avoid a specific virus — so they download after hours and still open up their organization to that risk. People are the low-hanging fruit when it comes to security."

Security managers say communicating with business units before establishing policies will ensure the policies created sync up with business processes — as well as increase the chances that the groups will follow the mandates.

"There is a key partnership you have to form with the business units so you can educate them and say, 'Look, don't e-mail this information, come to us and we'll help you figure out ways that you can exchange this information,'" said Beth Cannon, CSO at investment banking and brokerage firm Thomas Weisel Partners in San Francisco. Setting policies on what can and cannot leave the company in electronic format is an important exercise between the CSO and users, she said.

"Determine what information may need to be exchanged — because maybe sometimes you don't need to send a Social Security number. And you definitely don't need to e-mail it in the clear. Maybe we have an expectation as IT people that everybody should just know that," Cannon said.

Adding technology

A security culture cannot depend on people and process alone. Technology available today helps automate policy enforcement, data collection and protection, and augment shops short on staff.

James Ballou, who heads security for Driscoll Children's Hospital in Corpus Christi, Texas, faces the challenge of securing new technologies such as wireless — which he deems critical for bedside patient care.

By adding Cisco's Security Monitoring, Analysis and Response Systems (MARS) to detect anomalies in network traffic, Ballou said he can better secure his network. With limited staff, the IS security specialist and [Health Insurance Portability and Accountability Act] security officer says he depends on vendor technology to provide information that would take him too long to decipher.

"MARS is looking at data from all different sources, gauging its potential risk and correlating that for me to help me determine, where did it come from, what do I need to do to mitigate the risk and how can I avoid this in the future," Ballou said. "HIPAA compliance requires a minimum standard of security for us to meet, but we want to operate on a higher level than that. I need proactive, consistent threat management and pre-programmed responses built into our system to mitigate issues."

Industry watchers say companies that start honing their security practices today will save money tomorrow. While most companies spend about 3% of their total IT budget on security, those that crank the investment up to around 8% will — within 18 to 24 months — spend less on total security expenditures, according to research firm Gartner.

TRACY POWELL

"HIPAA compliance requires a minimum standard of security for us to meet, but we want to operate on a higher level than that."

James Ballou, IS security specialist and HIPAA security

"Security today requires organizations to raise the culture of IT to do things more securely, not to change how others work," said John Pescatore, lead security analyst at Gartner. "Expecting end users to think about security in the way that IT needs to will fail. End users shouldn't have a choice when it comes to operating more securely; the network, systems, IT team should make those decisions, and they should be transparent to end users."

Some first steps Pescatore recommends include updating systems to Simple Network Management Protocol Version 3, encrypting all e-mail to reduce the risk of data leaks and leaning on software vendors during licensing negotiations to prove their products are secure. "If you make your equipment more secure, if you have more secure systems, then you won't have to deal with as many issues and invest in more technology," he said.

On the vendor front

Cisco and Microsoft used the event to announce they will make their network access-control products interoperable by the delivery of Vista Server next year, an example of how vendors are increasingly willing to make sure their products work together to secure customer networks.

The agreement would have Cisco gear working with Microsoft systems to screen devices attempting to access a network. Industry watchers say the partnership is a sign of things to come.

"There has been a shift in Cisco over the past few years. The company is not as hell-bent on doing everything themselves; they are partnering more, and especially in the area of security," Yankee Group's Kerravala said.

Cisco CEO John Chambers, who delivered a keynote address at the show, described IP mobility and collaboration technologies as one of the largest IT security challenges facing enterprises, and possibly one of the greatest tools for converging physical and digital security.

Chambers outlined the benefits of "quad-play" — the combination of data, voice and video with mobility — and the security challenges associated with having a mobile workforce that accesses, shares and spreads data and information via a growing number of IP-enabled devices and across multiple networks.

"The opportunity for harm, either by deliberate action, or by neglect, becomes much higher," as an enterprise workforce has easier access to data, and the ability to share information easily via IP communications, Chambers said.

That opportunity for harm may translate into an opportunity for Cisco to make money in the security market with products and partnerships, but it also means customers can hope to see more integration among Cisco and other vendors — as well as interoperability efforts within the vendor community as a whole — when it comes to securing their gear and systems against internal and external attacks.

"The vendors are starting to hear the cries from their customers that they don't have just one vendor in their environment and those they do have need to do the work on integrating security and other functions and making it easier for the customer to deploy," Gartner's Pescatore said.

Senior Editor Phil Hochmuth contributed to this story.

Read Editor in Chief John Dix's column from the show. Page 36.

_INFRASTRUCTURE LOG

_DAY 18: Everything is frozen. It's our processes. They're inflexible. We can't respond to change.

_Why did we lock ourselves in like this? Brrrr.

_DAY 19: A way out. IBM WebSphere middleware for Business Process Management. It lets us streamline business tasks. We can test our processes before we roll them out and monitor performance once they're deployed, and reuse is easy because it's based on a service oriented architecture.

_Everything's unfrozen now. Wow, it's good to feel my toes again.

Take the BPM with SOA Assessment at:
IBM.COM/**TAKEBACKCONTROL**/PROCESS

VON

continued from page 1

- $500 million in IP phone sales in the same quarter this year.
- 100 million registered users of Skype, a 92% increase from a year ago.
- $2.5 billion spent on carrier VoIP gear in 2005, a 50% increase.

In contrast with the grandiose numbers, small businesses will be the focus of many product launches. Vendors also are targeting offices with several new all-in-one IP PBX boxes aimed at sites with five to 100 employees. Also expected are an array of tools to help companies manage and control VoIP traffic on the LAN and WAN, and wirelessly.

Viola Networks plans to launch its NatAlly Lifecycle Manager 5.1, a VoIP management and monitoring appliance that features a new service-level agreement (SLA) index feature. The SLA index lets users measure the voice quality of groups of IP phone calls or PC softphone calls from a particular site — such as a remote office connected via a WAN, or a specific LAN subnet with a departmental phone group. Unlike past Viola appliances, which could measure overall VoIP quality or individual-phone voice quality, the SLA index gives managers a more accurate view of call quality and potential network trouble spots that may affect VoIP calls, the company says. The box starts at $1,200.

Also on the management front, Apparent Networks is announcing a partnership with Nortel, in which Apparent's AppCritical VoIP network-management software will be bundled and integrated with Nortel's line of large enterprise and small-office IP PBX platforms — which include the Succession Communication Server 1000 and the Business Communications Manager. The AppCritical software provides network assessment and fault detection to a Nortel-based VoIP infrastructure, without agent software needing to be installed on IP phones, gateways or other gear.

Covergence is introducing a new Session Initiation Protocol management device that trunks SIP traffic through firewalls and across IP networks. The Eclipse CX-50 is a smaller version of the company's previous gear and economically enables SIP support in small offices. Previous boxes were designed for data centers. Eclipse devices also handle SIP signaling and media encryption, virus scanning, QoS control and identity-based access control, among other features. Pricing has not yet been released.

The device is intended to trunk calls between SIP-based IP PBXs while maintaining QoS to ensure voice quality and encryption to maintain privacy. It can perform these functions between PBXs and Microsoft Live Communications Servers as well.

The company also is announcing interoperability between its gear and Linksys VoIP routers to encrypt and authenticate VoIP generated by small and home offices.

Another small-and-midsize business-focused vendor, Allworx — which lists Versace, John Deere and the Red Cross among its customers — is launching its SIP-based 24x IP PBX product, aimed at sites with as many as 100 users. The device includes ports for an an integrated T-1/PRI voice circuit, and an Ethernet port for connecting to IP-based services. The 24x has basic, small-office telephony features (conferencing, hold, transfer, multiline support), as well as an integrated e-mail and Web server. The 24x box starts at $2,000 for 24 users.

Senior Editor Tim Greene contributed to this story.

Up with VoIP

6.9 million new VoIP subscribers were added in the second quarter of 2006, and carriers took in

$607 million

in VoIP services revenue in the same quarter.

SOURCE: TELEGEOGRAPHY RESEARCH

IT staff needs to sell security

BY TIM GREENE

ATLANTA — The focus of network security should shift from safeguarding infrastructure to protecting data, and that requires extraordinary marketing measures by IT security staff, according to speakers last week at the Forrester Research Security Conference.

Security is such an important issue for Diageo, the parent company for Smirnoffs, Guinness, Bailey's and other brands of alcoholic beverages, that the company has sophisticated, internal marketing videos to promote data security, said Claudia Nadenson, the company's CISO, who spoke at the conference.

In addition, the company sponsors educational sessions tailored to the regional culture of the branch being trained, Nadenson said. For instance, in Jamaica, where the company owns the Red Stripe beer brand, seminars are held at beach parties with boom-box music. Workers in the United Kingdom, on the other hand, respond better to a county-fair atmosphere, where workers walk from booth to booth for briefings, she said.

And prizes work. "We're not averse to giving away iPods if you can recite key areas of a policy. Our team says we are the corruption and bribery team," she said.

Publicized security breaches can damage corporate brands, she said, so it is important to prevent them. Because some of these breaches can be caused by business-unit workers who don't appreciate security, it is imperative that they understand the importance of policies, she said.

"The focus should be, we need to protect data vs. secure the infrastructure," said Paul Stamp, an analyst for Forrester. Stamp said to head off data leaks, business units must accept responsibility for the security of the data they generate and control. "IT people are data custodians, not owners," Stamp said. "We need to transfer responsibility to business people."

To do that, finance, marketing, human resources and other business departments have to perceive IT security as enabling their jobs, not as preventing them from using potentially productive IT tools, Nadenson said.

She suggests meeting with department heads and listening to their biggest business priorities first, then presenting security as an important element they should incorporate in new projects as they develop them. These meetings should be ongoing to keep security an important part of the process, Nadenson said. "It's about embedding security in the culture," she said.

In addition, IT executives need to quantify how well the internal security-marketing is working. "It's not about how many people were put through awareness training, it's about how they've changed the way they work," she said.

In two years at Diageo, Nadenson says the company has reduced the number of corporate laptops leaving the building. That action was needed to protect such sensitive data as projected earnings or the next promotion for a new drink.

The budgets for these efforts should come from the business units or from corporatewide budgets, she says. ■

Selling security

Claudia Nadenson, CISO for Diageo, says the company has sophisticated, internal marketing videos to promote data security. She suggests these ways to succeed in raising security awareness:

- Demonstrate how security is vital to the success of business initiatives.
- Suggest the technical help you can offer.
- Always deliver on that help.
- Follow up to say, "This is what we've done for you." Be a spin doctor for yourself.

NETWORKWORLD

EDITORIAL DIRECTOR: JOHN GALLANT
EDITOR IN CHIEF: JOHN DIX

■ NEWS

EXECUTIVE EDITOR, NEWS: BOB BROWN
NEWS EDITOR: MICHAEL COONEY
NEWS EDITOR: PAUL MCNAMARA

■ NET INFRASTRUCTURE

SENIOR EDITOR: JOHN COX (978) 834-0554
SENIOR EDITOR: TIM GREENE
SENIOR EDITOR: PHIL HOCHMUTH
SENIOR EDITOR: ELLEN MESSMER (941) 792-1061

■ ENTERPRISE COMPUTING

SENIOR EDITOR: JOHN FONTANA (303) 377-9057
SENIOR EDITOR: DENI CONNOR (512) 345-3850
SENIOR EDITOR: JENNIFER MEARS (520) 818-2928

■ APPLICATION SERVICES

SENIOR EDITOR: CAROLYN DUFFY MARSAN, (317) 566-0845
SENIOR EDITOR: ANN BEDNARZ (612) 926-0470
SENIOR EDITOR: DENISE DUBIE
SENIOR EDITOR: CARA GARRETSON (240) 246-0098

■ SERVICE PROVIDERS

SENIOR EDITOR: DENISE PAPPALARDO, (703) 768-7573
MANAGING EDITOR: JIM DUFFY (716) 655-0103

■ NET.WORKER

EDITOR: JOHN DIX

■ COPY DESK/LAYOUT

MANAGING EDITOR: RYAN FRANCIS
COPY CHIEF: TAMMY O'KEEFE
SENIOR COPY EDITOR: JOHN DOOLEY
COPY EDITOR: BOB SPRAGUE
COPY EDITOR: CAROL ZARROW

■ ART

DESIGN DIRECTOR: TOM NORTON
ART DIRECTOR: BRIAN GAIDRY
SENIOR DESIGNER: STEPHEN SAUER
ASSOCIATE DESIGNER: ERIC ANDERSON

■ FEATURES

FEATURES EDITOR: NEAL WEINBERG
SENIOR MANAGING EDITOR, FEATURES: AMY SCHURR
OPINIONS PAGE EDITOR: SUSAN COLLINS

■ CLEAR CHOICE TESTS

EXECUTIVE EDITOR, TESTING: CHRISTINE BURNS, (717) 243-3686
SENIOR EDITOR, PRODUCT TESTING: KEITH SHAW, (508) 490-6527
LAB ALLIANCE PARTNERS: JOEL SNYDER, Opus One; JOHN BASS, Centennial Networking Labs; BARRY NANCE, independent consultant; THOMAS POWELL, PINT; Miercom; THOMAS HENDERSON, ExtremeLabs; TRAVIS BERKLEY, University of Kansas; DAVID NEWMAN, Network Test; CHRISTINE PEREY, Perey Research & Consulting; JEFFREY FRITZ, University of California, San Francisco; JAMES GASKIN, Gaskin Computing Services, MANDY ANDRESS, ArcSec; RODNEY THAYER, Canola & Jones; SAM STOVER, independent consultant
CONTRIBUTING EDITORS: DANIEL BRIERE, MARK GIBBS, JAMES KOBIELUS, MARK MILLER

■ NETWORKWORLD.COM

EXECUTIVE EDITOR, ONLINE: ADAM GAFFIN
SITE EDITOR: JEFF CARUSO, (631) 584-5829
SENIOR ONLINE NEWS EDITOR: LINDA LEUNG, (510) 768-2808
MULTIMEDIA EDITOR: JASON MESERVE
ASSOCIATE ONLINE NEWS EDITOR: SHERYL HODGE
SENIOR ONLINE GRAPHIC DESIGNER: ZACH SULLIVAN

■ SIGNATURE SERIES

EDITOR: BETH SCHULTZ, (773) 283-0213
EXECUTIVE EDITOR: JULIE BORT (970) 482-6454
COPY EDITOR: TAMMY O'KEEFE

EDITORIAL OPERATIONS MANAGER: CHERYL CRIVELLO
OFFICE MANAGER, EDITORIAL: GLENNA FASOLD
EDITORIAL OFFICE ADMINISTRATOR: PAT JOSEFEK
MAIN PHONE: (508) 460-3333
E-MAIL: first name_last name@nww.com

ScriptLogic offers desktop-security tools

BY JOHN FONTANA

Desktop management vendor ScriptLogic is expected next week to add controls for securing USB and other ports on desktop computers so administrators can better protect the collection and dissemination of corporate data.

Desktop Authority 7.5 has an optional USB and Port Security feature that lets companies selectively lock out or permit the use of USB devices, including cameras, external hard drives, and DVD and CD burners.

"We have a number of applications that do require some usage of USB ports, and before, we could not monitor who needed those ports," says Jim Clements, consultant for special projects with the city of Raleigh, N.C."Now we can selectively allow cameras that are part of videoconferencing, but we can eliminate the use of memory sticks."

Clements says his only option previously was to shut everything down by disabling the USB features in the system's basic input/output system or allow everything to connect by keeping the port open.

The software also has updating capabilities, which allow scheduled and unscheduled desktop-configuration changes, and new deployment and management capabilities, including integration with ScriptLogic's Desktop Authority MSI Studio (formerly Installer Design Studio), which creates packages used to install software on desktops. The company plans to provide users all the tools needed to provision, manage and decommission networked desktops.

The USB/Port control is a policy engine that lets users create and assign policies based on individual or groups of users, or groups of machines. The feature supports nearly 20 devices, including PC Card devices, MP3 players, PDAs, smart phones, modems, and FireWire and Bluetooth devices, and works with the upcoming release of Microsoft Vista, as well as older Windows operating systems.

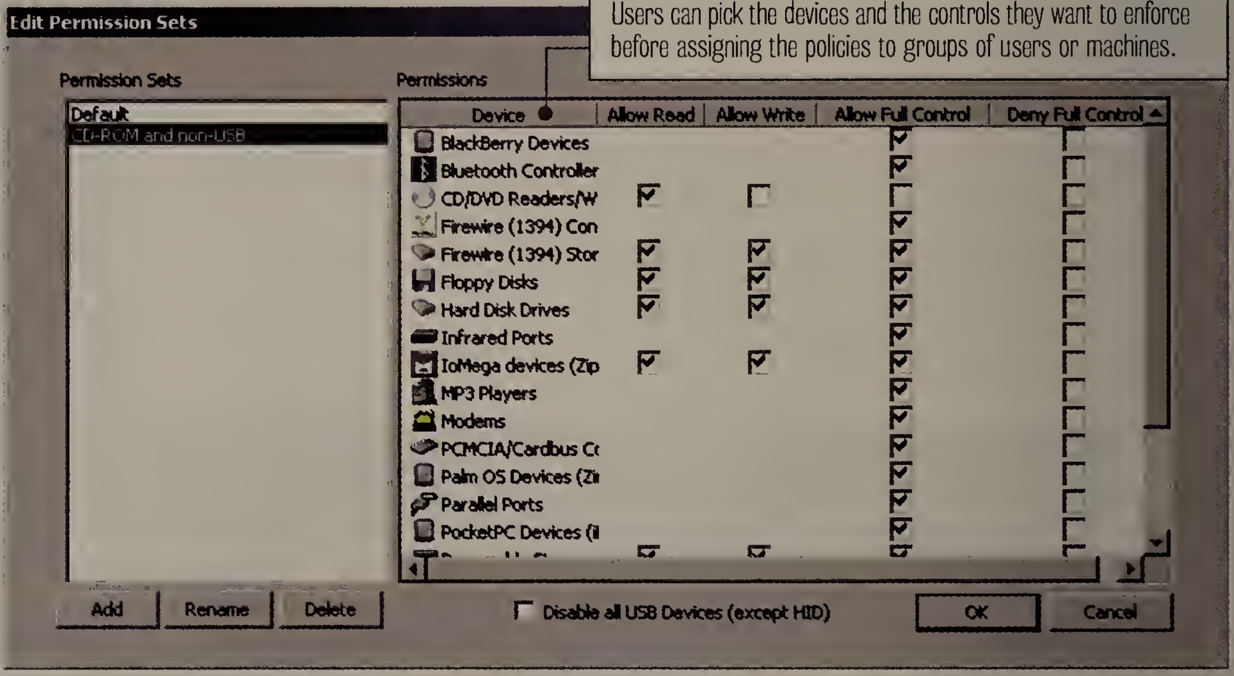
Also new in Version 7.5 is a refresh feature for updating or reinforcing the configurations and policies mandated for a desktop. Previously, those configurations could be altered only at logon or logoff, but now users can push out updates at any time and can run one-time updates.

ScriptLogic has added a point-and-click feature for deploying, updating and removing software from a desktop. Integration with MSI Studio lets users populate the Desktop Authority repository with software in the form of installation packages, so they have a management console from which they select a package to install and designate which Desktop Authority installation server will deliver it.

ScriptLogic's Desktop Authority 7.5, which competes with products from Altiris, LANDesk and Microsoft, is available at $38 per user. The optional USB and Port Security feature is priced at $10 per user. ■

Lockdown

ScriptLogic has updated its Desktop Authority desktop-management software with features for controlling use of USB and other ports.



Users can pick the devices and the controls they want to enforce before assigning the policies to groups of users or machines.

Edit Permission Sets

Permission Sets: Default; CD-ROM and non-USB

Permissions

Device	Allow Read	Allow Write	Allow Full Control	Deny Full Control
BlackBerry Devices			☑	☐
Bluetooth Controller			☑	☐
CD/DVD Readers/W	☑	☐	☐	☐
Firewire (1394) Con			☑	☐
Firewire (1394) Stor	☑	☑	☑	☐
Floppy Disks	☑	☑	☑	☐
Hard Disk Drives	☑	☑	☑	☐
Infrared Ports			☑	☐
IoMega devices (Zip	☑	☑	☑	☐
MP3 Players			☑	☐
Modems			☑	☐
PCMCIA/Cardbus Cc			☑	☐
Palm OS Devices (Zi			☑	☐
Parallel Ports			☑	☐
PocketPC Devices (i			☑	☐

☐ Disable all USB Devices (except HID)

AirMagnet updates WLAN site survey

Software syncs up with Google Earth for mapping of wireless access points.

BY JOHN COX

AirMagnet has released a version of its wireless LAN mapping application that includes a companion program for creating and refining the initial WLAN design.

Also new with AirMagnet Survey 4.0 is an interface with satellite photo data drawn from Google Earth, and an improved wireless spectrum analyzer that can detect and identify interference caused by radios outside the 802.11 standard, such as microwave ovens or Bluetooth devices.

Overall, the changes are intended to make the laptop application a more accurate and comprehensive design, planning and monitoring tool for indoor and outdoor Wi-Fi networks. A network administrator runs Survey on an Windows XP or 2000 laptop and collects radio data via the laptop's wireless network interface card by walking or driving around a site.

nww.com

Wireless LAN security Buyer's Guide

Find detailed product information on wares that add security to WLAN environments. Check out our online Buyer's Guide.

www.nwdocfinder.com/4058

Most WLAN vendors, such as Aruba Wireless Networks, Cisco and Trapeze Networks, have at least basic site survey and planning tools. Third-party rivals include Ekahau and Wireless Valley (now part of Motorola).

The previous edition of Survey worked with an image or file of a building's floor plan. A user walked around the building with the laptop and Survey to collect access point data, including their locations. This information was then associated with icons overlaid on the floor plan, showing channel assignments, the signal strength of the access points, link speeds with wireless clients, the actual radio coverage throughout the building and other data.

The new application, Planner, can run on its own or as a companion to Survey. On its own Planner lets a user design a network model of what the initial WLAN would look like based on answers to questions about the structure's layout, the building materials in its construction, user requirements and so on. Planner suggests locations for access points and a channel assignment plan.

As a companion to Survey, Planner then can use the real-time data collected by Survey, factor this into the design and let users compare the original design with the actual performance of the WLAN.

The combination of tools lets users accurately decide about capacity planning, about whether the WLAN can support voice or video applications and about the effect of increased numbers of users on the network's performance, according to Wade Williamson, product manager for AirMagnet.

Planner includes a catalog of performance characteristics of about 90 commercially available antennas. Users can select different antennas, such as a directional antenna with a specific energy pattern, to see what affect that choice will have on coverage, range and signal strength.

As for the new version of AirMagnet Survey, users can now work with Google Earth images by driving through an area with their wireless laptops and, optionally, a GPS device linked via USB port to the laptop and that feeds satellite coordinates to the Survey software. Survey picks up information about WLAN access points active in that area. Later, users download an area image from Google Earth, and the software maps the access point data to the Google image, creating an accurate visual map of Wi-Fi coverage and performance.

AirMagnet Planner costs $2,000 as a separate product. Bundled with Survey, the price drops to $1,000

Version 4.0 of AirMagnet Survey standard edition is priced at $2,000. The more advanced Survey Pro edition, which includes the improved Spectrum Analyzer, GPS support and the Google Earth interface, among other added features, costs $3,600. ■

Cisco airs low end of big router line

BY PHIL HOCHMUTH

Cisco last week launched the smallest version yet of its biggest router. The four-slot Carrier Routing System-1 is intended to extend 40Gbps from a core network to regional carrier locations.

The four-slot CRS-1 joins its eight- and 16-slot brethren and offers carriers another tool for expanding 40Gbps, or OC-768, connectivity throughout a network. The device includes four slots that can support four-port OC-192 (10Gbps) line cards, or single-port 40Gbps blades. The box also includes several traffic-shaping and network-virtualization features aimed at serving business and consumer network customers, Cisco says.

The four-slot CRS-1 supports as much as 320Gbps of total routing capacity, Cisco says. Traffic management features in the router also let users carve up bandwidth or network services for various customers, with Secure Domain Routers. This feature lets users create a virtual router for each line card in a CRS-1 system.

The traffic on virtual Secure Domain Routers is segregated from other network segments, keeping customers' data from mixing, and enabling carriers to apply different rules to traffic and use different protocols and technologies for customer networks.

The smaller-size CRS-1 also can operate with CRS-1 chassis in Cisco's multichassis routing configuration, which lets multiple CRS-1 boxes be lashed together for greater failover and distributed router processing capabilities, Cisco says.

The four-slot CRS-1 is scheduled to be available in November, starting at $160,000. ■

WAN optimization's newest player: Cisco

Company delivers acceleration, optimization technologies for customers consolidating branch office systems.

BY DENISE DUBIE

Cisco last week threw its hat into the crowded WAN optimization ring when it unveiled a set of products designed to boost corporate application performance over WANs.

Cisco Wide-Area Application Services (WAAS) combine the company's existing technologies — such as Wide-Area Application Engines (WAE), Wide-Area File Services (WAFS) and Application and Content Networking System (ACNS) software — to provide customers a suite that can accelerate application traffic, speed large data transfers and optimize WAN performance. WAAS also include WAFS technology that Cisco acquired with Actona in 2004 and incorporate technologies such as TCP and HTTP optimization, caching and compression from various groups within Cisco.

The WAAS technology is software delivered on a variety of Cisco's data center and branch office appliances: the WAE-7326 for data centers, and the WAE-612, WAE-512 and NM-WAE for branch offices. With the NM-WAE, the company also designed WAAS to fit into existing Cisco gear.

Cisco earlier this year announced its Application Control Engine, a blade that resides in a switch deployed between a server and the WAN to speed application delivery. WAAS now include the NM-WAE module, which fits into Cisco's 2800 and 3800 Integrated Services Routers (ISR). WAAS products plug in to the network — with devices installed at the data center and in the branch office to enable technologies such as compression — and can be configured with various administrative and access rights for IT managers, depending on their job description, Cisco says.

Harold Hamm, vice president of IT and telecommunication at Reynolds, Smith and Hills, an architecture and engineering firm in Jacksonville, Fla., says he beta-tested the WAAS appliances in four locations between April and July because users had been challenged to work on large files at disparate offices. He had balked at what seemed like good technology from Packeteer and Riverbed because he didn't want to hinder the QoS policies he had in place with Cisco IP phones and because he had Novell file and print servers.

"If end users were working on a design, the cursor sometimes would be in the wrong place because the file transfer was so slow," he says. "We wanted something to speed that up without changing our entire environment."

With T-1 lines to 17 design offices and 25 project locations, Hamm says file transfer rates became a major issue. Cisco WAAS let him speed up data transfers and make working on a project at separate locations possible. Files could be 20MB to 100MB and more, he says, so he needed a technology that let the T-1 lines handle that traffic at faster speeds.

"It could still be faster, and I think Cisco will work on that in coming releases, but I like that the technology doesn't sit in line of the network and that it makes working on large files more than just bearable for our end users," Hamm says.

While he would like to see Cisco increase the speed of transferring large files — the initial file transfer is about three times faster than in the past, with follow-on access being much quicker because content is cached locally — Hamm says he plans to invest in WAAS and become fully deployed across 17 design locations by this time next year.

WAAS are Cisco's entry into the bustling WAN optimization market, which includes competition from Expand Networks, F5 Networks, Juniper Networks, Riverbed and others. Protocol optimization, caching, content distribution and streaming media technologies are among the features Cisco included in WAAS. Cisco says the technology will let customers consolidate distributed servers and storage into centrally managed data centers. Analysts say it's about time.

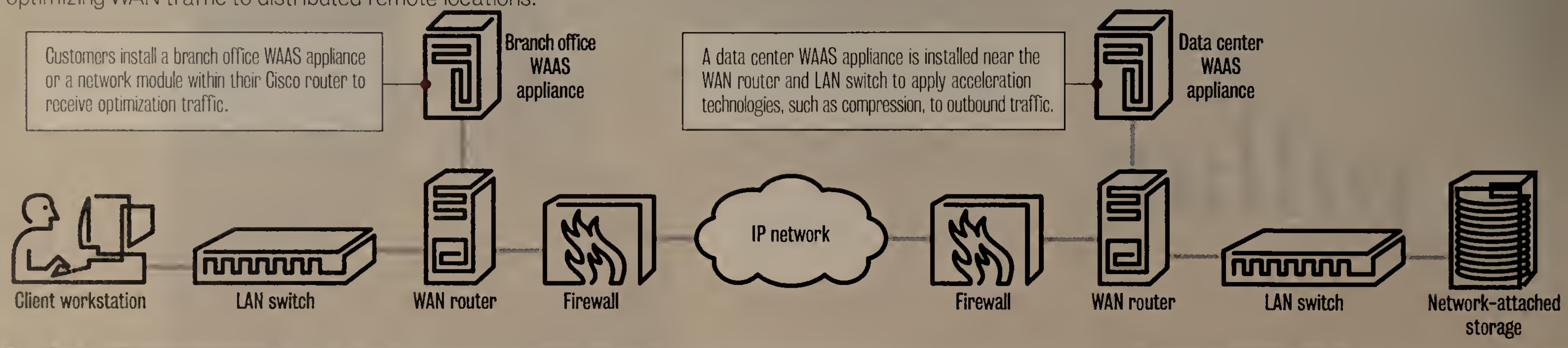
"It is significant because Cisco is finally entering the market with a product that appears to be very competitive," says Joe Skorupa, a research vice president at Gartner. And Cisco's network manager customers could welcome WAN optimization technology from a known vendor.

"With WAAS, Cisco also offers a way to

See Cisco, page 24

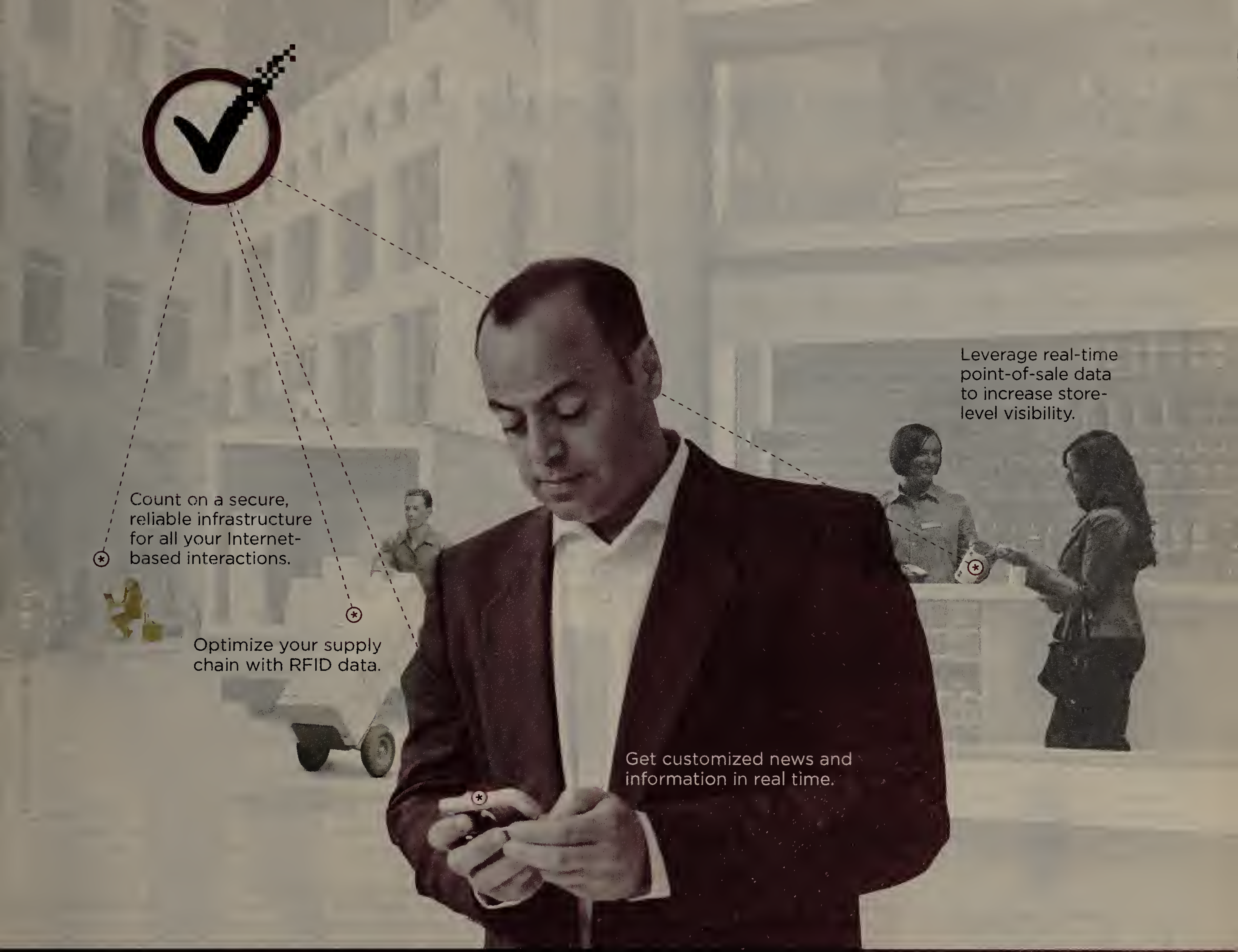
Cisco to the branch

Cisco Wide-Area Application Services (WAAS) products use data center and branch office appliances to deliver software for compressing, caching and optimizing WAN traffic to distributed remote locations.



Customers install a branch office WAAS appliance or a network module within their Cisco router to receive optimization traffic.

A data center WAAS appliance is installed near the WAN router and LAN switch to apply acceleration technologies, such as compression, to outbound traffic.


Count on a secure, reliable infrastructure for all your Internet-based interactions.
Optimize your supply chain with RFID data.
Leverage real-time point-of-sale data to increase store-level visibility.
Get customized news and information in real time.

Aruba CEO says WLANs break security model

BY JOHN COX

Aruba Networks CEO and President Dominic Orr says enterprise wireless LANs are about to get much less interesting.

That's because the increasing commoditization of WLAN gear, along with the advent of the 100+Mbps 802.11n standard, will make wireless connectivity a routine part of the enterprise network infrastructure.

But what won't be routine is the challenge WLANs have created to the traditional conventions and architectures for network authentication and security.

"The security architecture for wired nets, based on using physical port-based conventions, won't work," Orr says. An industry veteran of such companies as HP, Bay Networks and Alteon, Orr took over the reins at Aruba in April. "You need specific, user-oriented identification, content and location data [to secure the net]," he says.

This is where the emerging enterprise battleground lies, according to Orr.

Boring WLANs

"WLAN is, if not dead, then uninteresting," he says. "Once it's 'spec-able' by the IEEE, most of the profit goes to the silicon makers. Eighteen months after 802.11n is standardized, the WLAN is no longer an interesting business. It's a very small window, and it's quickly being commoditized."

But it creates a huge hole in the traditional enterprise security model, which assumes the person at the far end of a wire linked to a specific switch port is the person who is supposed to be sitting at that desk.

> "The security architecture for wired nets, based on using physical port-based conventions, won't work."
>
> *Dominic Orr, CEO and president, Aruba Networks*

What's needed is secure mobility as a logical add-on to the enterprise network, he says. This will become increasingly urgent as more enterprise workers become mobile. Today, only about 5% of workers are mobile, but that will rise to more than 20% in two or three years, Orr says.

Most WLAN innovation has been at Layers 1-3, focusing on wireless Ethernet connectivity, according to Orr. Aruba is focusing on Layers 4-7 in its line of WLAN controllers and companion thin access points. "Our goal is mobile access control: Who is this person [on the wireless link], what is his role in the organization, what device is he using, what applications?" Orr explains.

One Aruba customer, which Orr wouldn't name, is a large consulting company that's spent more than a $1 million on Aruba products. But the customer has no wireless connectivity. Instead, it's using Aruba controllers on the wired network to create and manage secure, authenticated, managed connectivity for visiting staff and clients, including a VPN link back to the client's home network.

"We create a mobile edge to the network," Orr says, citing one of Aruba's marketing terms. "We are front-ending the network for network access control, security, authentication, user privileges. You want the network infrastructure to recognize the user, his role and profile, and then treat him accordingly."

In addition, he says, there is no network reconfiguration needed at Layers 1 and 2, and Aruba can work with whatever network access control scheme — such as from Cisco or Microsoft — that the enterprise decides to adopt.

Vendors attack

Aruba executives say they're not worried that network vendors such as Cisco and security vendors such as Check Point are attacking this issue in different ways.

Orr, who has competed with Cisco for years while with Alteon, Nortel and other companies, is almost dismissive of the network giant. Cisco's WLAN focus is on connectivity.

"They're all Layer 1 and 2 networking devices," he says. "Cisco has initiatives in security, content networking and connectivity technologies. We just don't see how this will all come together."

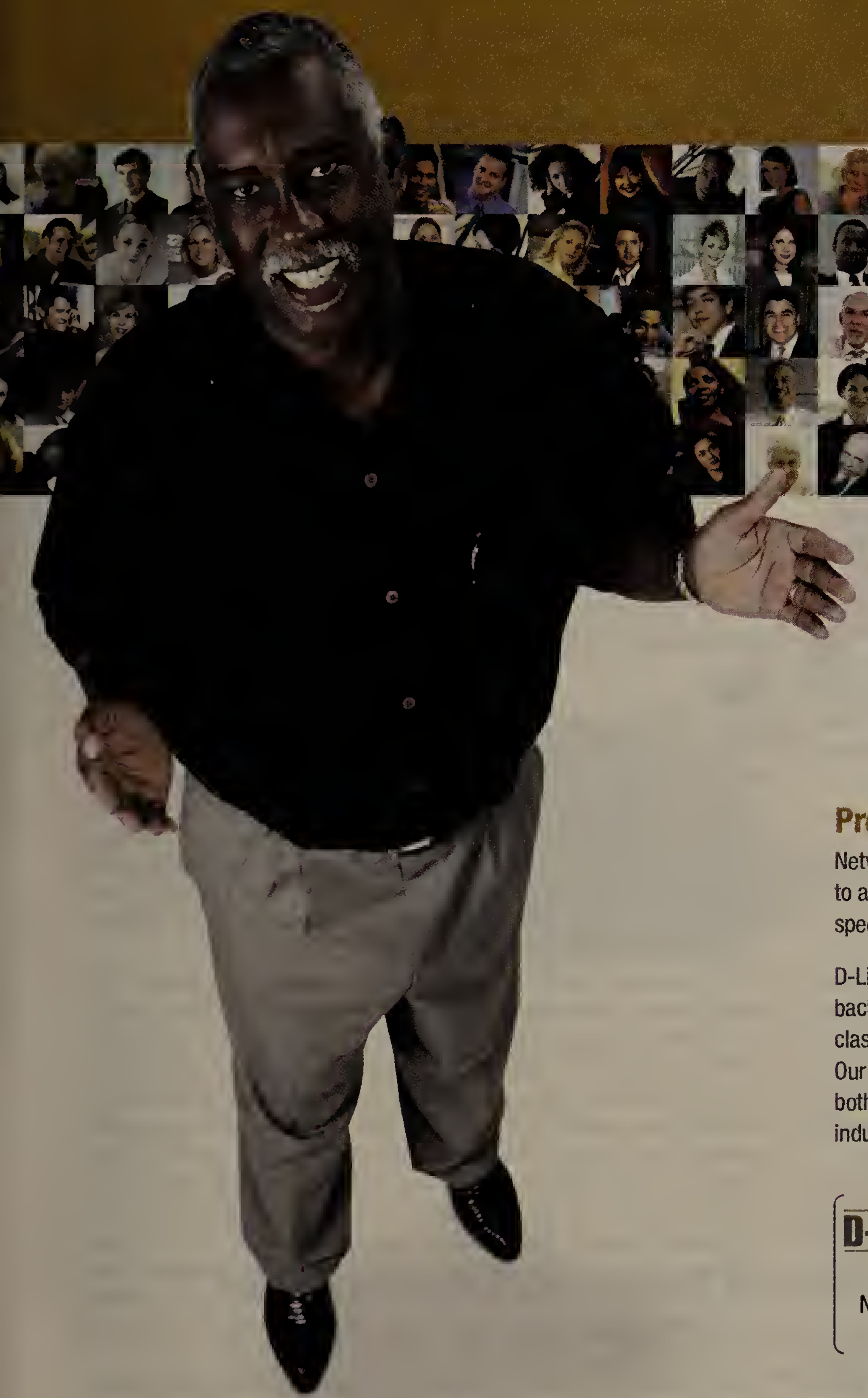
But the critical constraint is that Cisco needs to grow total revenue by $4 billion per year in incremental business to maintain a stock price roughly in the area of $20 per share. "Gigabit Ethernet to the desktop, whether you need it or not, and VoIP . . . these are the kinds of big network upgrades that are being pushed by Cisco," he says.

Network security vendors are addressing user-oriented security issues, says Keerti Melkote, Aruba's vice president of marketing. But they remain focused on fixed clients — wired desktops. Most of these solutions require placing a small agent program on each client, something he says most companies will find unacceptable.

To exploit this opportunity, privately held Aruba is taking the first steps toward an initial public offering. According to Orr, this means setting in order its finances and government compliance over the next two months, and then timing the offering.

Aruba has an annual run rate of just more than $100 million, Orr says. It is sometimes profitable, depending on changing decisions of how much of that income to reinvest in different areas of the business. ■

Millions Connected. Millions Saved. It's Your Turn.



See Why More & More Businesses are Switching to D-Link

"The State of Louisiana entrusts us with sensitive information. We trust D-Link® NetDefend™ and switching to keep our data and communications secure."

-Collis Temple, CEO
Harmony Center, Inc.

Proven Enterprise-Level Networking & Security is Now Within Your Reach

Network security is no longer a luxury. But you can't afford to have your security solution grind your productivity to a crawl, either. Harmony Center, Inc. chose D-Link switching and security solutions to get both protection and speed — affordably.

D-Link provides End-to-End Solutions for Small and Medium Business. The switches that make up your network backbone, advanced firewalls and Virtual Private Networks (VPN), Network Attached Storage (NAS), business-class wireless — D-Link wants to be your IT vendor of choice, and we believe we have earned that consideration. Our products match-up feature for feature, and as a true designer and manufacturer we are in direct control of both quality and costs. That means you get the highest-quality products with the most aggressive pricing in the industry. **Connections Made. Money Saved. Period.**

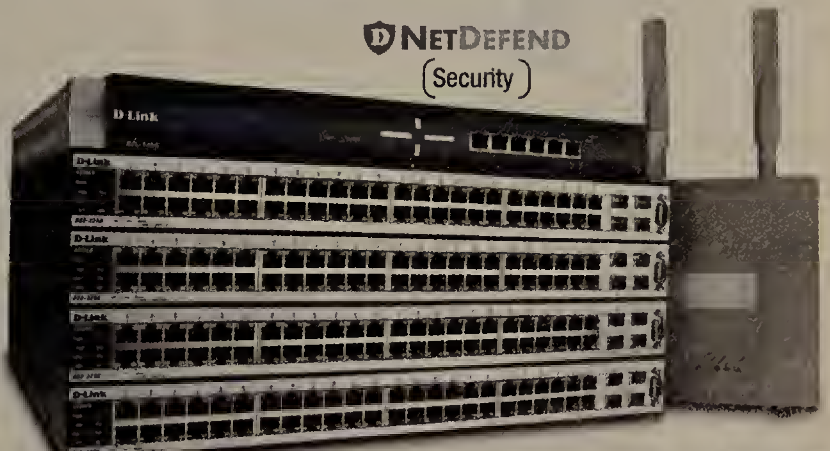
D-LINK@WORK™
End-to-End
Networking Solutions for
Your Growing Business

BUILDING NETWORKS FOR PEOPLE
20
D-Link
1986-2006
Twentieth Anniversary

D-Link celebrates 20 years of networking excellence. Limited time savings on over 300 products!

Learn more at www.dlink.com/at-work

or call 1-888-XSTACK1



NETDEFEND
(Security)

AirPremier
(Wireless)

XSTACK
(Switching
IP Telephony
Network Storage)

Trust the Global Leader in SMB Connectivity

END TO END SOLUTIONS
From the core, to the edge, to wireless switching: D-Link provides **complete end-to-end networking solutions** for your business D-LINK@WORK

MARKET LEADERSHIP
Shipping more than 100,000 connections a day worldwide, D-Link is the **market share leader** in SMB connectivity[1] In-Stat

PRODUCT EXCELLENCE
Put your trust in a true designer and manufacturer that's been delivering **excellence in engineering** for two decades ISO 9001

Market Share information derived from In-Stat Q2 2006 Wireless LAN Equipment, Ethernet LAN Switch and Broadband Equipment Market Share Reports. Prices and specifications are subject to change without notice. D-Link, the D-Link logo, NetDefend, AirPremier and xStack are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States and other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies. Copyright © 2006 D-Link Corporation/D-Link Systems, Inc. www.dlink.com

D-Link
Building Networks for People

Selling books by giving them away

NET INSIDER

Scott Bradner

Ross Anderson (www.nwdocfinder.com/5143 and /5144) is one of the more interesting security folks writing these days. He is a professor of security engineering at University of Cambridge (the other Cambridge) Computer Laboratory and seems to come up with new and useful perspectives on a wide range of security-related topics.

I particularly recommend "Why Information Security is Hard — An Economic Perspective" (www.nwdocfinder.com/5145), a 2001 paper detailing the economic reasons that people and companies do not always have the incentive to make the world safer. Ross wrote *Security Engineering*, one of the best security books around. He now has put the book online for free download (www.nwdocfinder.com/5146), even though it's still for sale. Ross, and I assume Wiley, the publisher of the book, are betting that making the book available for free will increase sales of the printed edition.

Ross explains his decision to put the book online at his Web site."My goal in making the book freely available is two-fold. First, I want to reach the widest possible audience, especially among poor students.

"Second, I am a pragmatic libertarian on free culture and free software issues; I think that many publishers (especially of music and software) are too defensive of copyright. I don't expect to lose money by making this book available for free: More people will read it, and those of you who find it useful will hopefully buy a copy. After all, a proper book is half the size and weight of 300-odd sheets of laser-printed paper in a ring binder." (I like the concept of a "pragmatic libertarian.")

Ross is far from the first person to think that making the text of a book available for free will increase sales. The U.S. National Academies, which advises the government on science, engineering and medical issues, has made its books available for reading and download online (at www.nap.edu/) for years. The National Academies is not as liberal as Ross is — it has perhaps the world's least user-friendly interface for reading the books online, while Ross just lets you download PDFs of the chapters. Maybe the Academies think that making it painful to read the books online will encourage purchases. Ross and Wiley demonstrate the more enlightened view that the content itself will be the selling tool.

Even with the awful user interface, the Academies is far better than most publishers, which seem to be petrified of the Internet for anything other than book sales. How else can you explain their lawsuits to stop Google's efforts to make it easy for people who might want to buy books to find which books they might want to buy? Google's Book Search (http://books.google.com/) has started making out-of-copyright books available for download, and Google wants to make all the books it can get searchable. Only excerpts of in-copyright books would be shown, so readers would have to find the book in a library or buy a copy if they wanted to read more than the excerpts.

Common sense would lead a person to believe that this could only be good for the publishers. Maybe they even could set up ways for on-demand printing of out-of-print books. I do not understand the publishers' "make the future go away" approach. Maybe Ross can come up with an explanation.

Disclaimer: Harvard has had a rather long time to understand that the future is rarely deterred, but the above book-selling advice is mine, not that of the university.

Bradner is a consultant with Harvard University's University Information Systems. He can be reached at sob@sobco.com.

Intel slashes workforce

BY JENNIFER MEARS

As expected, Intel last week said it would slash 10,500 jobs, or about 10% of its workforce, by the middle of next year as the chip maker attempts to regain its footing in an increasingly competitive x86 processor market.

The cuts, which come as part of a broad company overhaul that Intel launched in April, are expected to result in savings of about $3 billion by 2008, company executives said.

Intel plans to cut 7,500 jobs by year-end, with reductions in management, marketing and IT functions. In June, Intel said it would shed its communications units to sharpen its focus on its core microprocessor business. In July, it announced it would lay off 1,000 managers.

The cuts will be more widespread in 2007 "as Intel improves labor efficiency in manufacturing, improves equipment utilization, eliminates organizational redundancies, and improves product design methods and processes," the company said in a statement.

"These actions, while difficult, are essential to Intel becoming a more agile and efficient company, not just for this year or the next, but for years to come," said Paul Otellini, Intel president and CEO, in the statement.

Intel, which dominated the x86 processor market with a more than 90% share just a few years ago, has seen Advanced Micro Devices (AMD) chip away at its lead. The smaller chip maker now holds about 26% of the market, according to the latest figures from Mercury Research.

"Intel got fat and comfortable," says Gordon Haff, an analyst at Illuminata.

While the cuts don't come as a surprise, the number of layoffs "is fairly aggressive," Haff says. He adds the job reduction is similar in many ways to the approach used by HP CEO Mark Hurd, who has improved the computer maker's financial performance with job cuts and other cost-cutting measures without drastically altering its overall strategy.

"Intel is really going after operating efficiency, rather than axing large areas of products," Haff says. This should be good news for enterprise buyers, because "more efficiency should translate to better prices over the long term," he says.

Intel has felt pressure from Wall Street in recent quarters. In July, it reported profits of $885 million for the second quarter, less than half of the $2 billion it reported in the same period a year ago (www.nwdocfinder.com/5131). Otellini has said he expects Intel's annual profit to be about $9.3 billion this year, down from the $12.1 billion it earned in 2005.

Intel blames a slowing PC market, as well as pressure from AMD, for its flagging sales.

"Intel has lots of things to do [to get back on track], but slimming, focusing and executing on its road map would be a good start," Haff says.

Already Intel is stepping up the speed at which it's getting products to market. It has begun shipping its new line of processors — including the Woodcrest Xeon (www.nwdocfinder.com/5132) and the Conroe desktop chip (www.nwdocfinder.com/5133) — that provide better performance and consume less power, characteristics that have helped push AMD's Opteron into a growing number of enterprise data centers. ■

Cisco

continued from page 20

implement WAN optimization using your existing routing and switching infrastructure, [which is] critical, because enterprise [companies] are trying to find ways of rationalizing how much infrastructure they should put in each branch," says Robert Whiteley, a senior analyst with Forrester Research. "There are the folks that have been literally waiting for Cisco to come out with a solution. Now the network Goliath is finally delivering."

As Cisco poses significant competition to existing optimization technology leaders, the company will not be without its challenges entering the crowded market, analysts say.

"The competition — Riverbed, Juniper, F5, Expand and others — are on their second or third generation of protocol-specific optimizations, so performance may not be equal. [Those competitors] have credible products and longstanding customer relationships," Skorupa adds. "Others such as Blue Coat, Stampede and ICT Compress offer innovative features like HTTPS acceleration, integrated media streaming and client-based software [WAN optimization controllers] that Cisco lacks."

Skorupa points out the company still needs to fully integrate WAAS with existing ACNS products, as well as prove the WAAS technologies can scale to "bigger networks and high bandwidth." It also may have to establish relationships with a different set of IT buyers.

"Cisco still lacks good contacts in the application departments that Citrix/Microsoft, F5, Juniper and Riverbed have. Cisco will find it easier to sell when the network teams, or possibly, the storage teams, take the lead. When servers or applications are in the lead, Cisco is in a less powerful position," Skorupa says.

Forrester's Whiteley agrees. WAAS success will depend partly on Cisco convincing IT shops that acceleration and optimization products belong in the network.

"Cisco needs to make sure it convinces people that this [technology] belongs in the network. Part of the reason Riverbed and others have done so well is because they don't sell directly to the network managers in the enterprise. Instead, they go after line-of-business owners, application owners or data center managers," Whiteley explains. "For Cisco to flex its muscle with network gurus, it must prove that its solution is just as effective as a module in an ISR router or a blade in a Catalyst switch — which is a unique value proposition that no other vendor can touch."

The WA-512 series appliance starts at about $8,500 and the NM-WAE starts at about $4,000 for Cisco ISR customers. Select WAAS products are generally available this week; the NM-WAE is set to ship by year-end. ■

SECURITY INSIDER

Mike Rothman

IBM legitimizes managed security

$1.3 billion is a lot of money. If traveling is your thing, you could buy 38 Gulfstream V jets to fly in style and even have a little left over for gas money, or 7,900 Bentley Continental GTs to make sure you (and all your friends) are comfortable at ground level.

IBM, however, hopes you'll take some of that coin, buy one Bentley and hire 10,000 IBM-ers to drive you around. Why drive yourself when they can do it for you?

That's what IBM's acquisition of ISS is all about: services. Sure, services were only 15% of ISS' revenue stream, but they were where most of its efforts have been. Never mind that those efforts were devoted to services because ISS was becoming less competitive in the product space. Never mind that its vaunted X-Force research team had been marginalized by more aggressive, more timely and better-marketed competitors, such as eEye, F-Secure and SiteAdvisor.

Never mind that ISS had missed revenue projections for three quarters running and it wasn't looking good for the rest of the year. Never mind those pesky details. ISS was drowning in a competitive sea of larger security players with bigger and better products and channels. Then IBM threw it a $1.3 billion life jacket. You'd figure with that much money stashed in the life jacket, it would sink like a stone — but I digress.

The fact is that IBM paid a tremendous amount of money, based on any kind of economic measure, especially when you consider the uncertain future of ISS' products. But the services opportunity is compelling.

I can paint a picture where users of all sizes look to someone else to do the grungy work of protecting their networks, data centers and applications. Of course, no user in his right mind should be outsourcing his security strategy, compliance reporting or communicating the security value proposition to the powers that be. That's always an inside job.

It's perfectly legitimate, however, to get someone else to manage the boxes that protect you from the bad guys. Why? In my best British accent: "It's economics, dear Watson. Economics." Managed security is all about economies of scale. For most users, making significant investments in all sorts of security management hasn't paid off. They don't have the scale to gain the leverage that makes sense.

Large managed-security companies would have that leverage. Given the scale of all the networks they manage, they can cost-effectively deploy technologies such as security information management and anomaly detection.

Because security events happen fairly infrequently (if you have your defenses up to snuff), you don't need your own dedicated band of merry men and women sitting around the table 24/7 waiting for something bad to happen. A big service provider can do that for you, and it can do it cheaper than you can.

It's also a maturity thing. Outsourcing disciplines usually take 10 to 15 years to become accepted. Yes, that long. Remember mainframe outsourcing? That took even longer, but now you are hard-pressed to find an enterprise that still manages its own Big Iron.

Networks have been the same way. Networks in the early '90s were all about private lines and multiplexers managed by the internal network people. Now we use frame relay and managed IP services. If something breaks, you call the service provider and yell at it.

I believe we'll see the same thing in network security: Someone else will manage those firewalls, intrusion-detection systems, antispam gateways and their brethren. Not today, and not tomorrow, but within a couple of years.

So, IBM made a long-term bet that managed security will be big, and it wanted to have a leadership position early. It's probably right. $1.3 billion is a big number, but when you amortize it over 10 years, it seems pretty manageable.

Rothman is president and principal analyst of Security Incite, an analyst firm focusing on information security. Read his blog at http://feeds.feedburner.com/securityinciterants or send e-mail to mike.rothman@securityincite.com.

VeriSign security service expanded for apps, databases

BY ELLEN MESSMER

VeriSign last week announced an expansion of its log-management service beyond firewalls, operating systems and intrusion-detections systems to collecting log data related to applications and databases.

VeriSign's service is based on its Security Defense Appliance, which is placed inside the corporate network to collect, analyze and store logs. VeriSign says it's expanding the log-management service to collect raw data or just the security-related events pertaining to applications and databases of corporate customers.

According to Gartner, several managed security service providers, including Lurhq, Internet Security Systems and Counterpane, also offer log analysis services.

"Centralized logging and monitoring of application-level events is being driven by regulatory compliance, highly publicized data theft incidents and targeted application-level attacks," says Kelly Kavanagh, Gartner analyst in information security and privacy.

Amrit Williams, a Gartner consultant who specializes in data-analysis tools, notes the choice between a corporation developing its own log-aggregation process or outsourcing to a service provider is often made in favor of a service provider because there are lower upfront costs.

VeriSign says its log-management services are used by 800 corporations to manage about 10,000 devices.

"We're adding applications and databases from a wide range of vendors, including Oracle, PeopleSoft, SAP and IBM, as well as custom applications," says Scott Magrath, director of product marketing in VeriSign's managed security services group. The company has entered a partnership to use technology from LogLogic to pull data from a broad range of systems.

According to Magrath, the raw data can be stored on a database on the customer premises or externally, including within VeriSign's data centers in Mountain View, Calif., or Herndon, Va. "They can see reports related to this data via our customer Web portal," he says. Alternately, data about applications and databases related just to security — such as an excessive number of failed log-on attempts — also can be stored by VeriSign.

"Anything we identify as a security event, we send that back to the security operation center and an employee notifies the customer," Magrath says. Corporations want to make a wide collection of log data to satisfy auditors, and "the biggest push for collecting of log data is to be in compliance with regulations of many kinds," he says.

The baseline price for VeriSign's log-management service ranges from six to seven figures annually, based on a monthly fee per device. ■

Silicon Valley Wi-Fi network contract goes to Cisco, IBM

BY JOHN COX

Cisco, IBM and two partners have been awarded the contract to build a public 802.11-based wireless mesh that is intended to blanket most of the Silicon Valley peninsula of California, some 1,500 square miles.

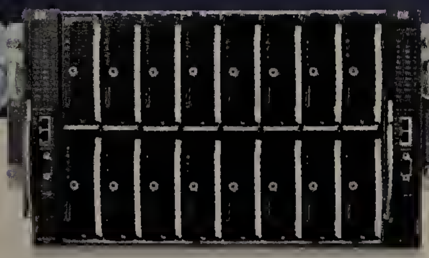
The network will have tens of thousands of wireless mesh access points, potentially offering access to 2.4 million residents in 42 peninsula communities. Cisco currently offers the Cisco 1500 dual-radio mesh product, first introduced about a year ago.

Cisco and IBM joined with Azulstar Networks, a Michigan municipal wireless networking company founded in 2002, and SeaKay, a California nonprofit group that organizes the use of digital technologies to improve social services in underserved communities in the San Francisco Bay Area. The quartet created a joint venture called Silicon Valley Metro Connect.

The venture now will start detailed contract negotiations, with an eye to starting the network rollout sometime in the fourth quarter, according to Alan Cohen, senior director, Cisco Mobility Solutions. Cohen says the network ultimately will support residential and business services, such as including voice and video in addition to data, distinguished by bandwidth and security. The network also will be the infrastructure for dedicated services to public safety, healthcare and other municipal departments.

IBM will act as the network designer and integrator.

The partnership will offer up to 1Mbps as a free base service, with an array of privacy protections. Wireless VoIP and video streaming will be fee-based services. In 2007, the partnership plans to deploy IEEE 802.16 WiMAX base stations for fixed and mobile wireless broadband users. ■



Chaos, now under your control.

HP ProLiant BL35p BLADE SERVER

with ProLiant Essentials Management Software

- Up to 2 Dual-Core AMD Opteron™ 200 Series processors
- High density: Up to 96 servers per rack
- Flexible/Open: Integrates with existing infrastructure
- HP Systems Insight Manager™: Web-based networked management through a single console
- Rapid Deployment Pack: For ease of deployment and ongoing provisioning and reprovisioning
- Integrated Cisco or Nortel switch options

HP BladeSystem servers offer tools to help you keep pace with fluctuating demands. The HP ProLiant BL35p Blade Server is designed to relieve some of the stress. Its AMD Opteron™ processors offer dual-processor power with breakthrough efficiency. With management features like the Rapid Deployment Pack that lets you deploy and redeploy blades without missing a beat, and a single-view, graphical user interface that streamlines monitoring and configuration, HP BladeSystem servers work with you so you don't have to work so hard. And, bundled with the StorageWorks MSA1500cs, you can reduce the cost and complexity of deploying a storage area network, giving you a better return on investment.

HP StorageWorks MSA1500cs

with StorageWorks Essentials Management Software

- Up to 24TB of capacity (96 250GB SATA drives)
- Up to 16TB of capacity (56 300GB SCSI drives)
- Ability to mix SCSI and Serial ATA enclosures for greater flexibility
- 2GB/1GB Fibre connections to host

SMART ADVICE > SMART TECHNOLOGY > SMART SERVICES

AMD 64 Opteron™

Call 1-888-223-5441
Click hp.com/go/bladesmag49
Visit your local reseller

hp invent

Reseller prices may vary. See Web site for full details. For hard drives, 1GB = 1 billion bytes. Actual formatted capacity is less. Photography may not accurately represent exact configurations priced. Associated values represent HP published list price. AMD, the AMD Arrow Logo, AMD Opteron and combinations thereof are trademarks of Advanced Micro Devices, Inc. ©2006 Hewlett-Packard Development Company, L.P.

EYE ON THE CARRIER

Johna Till Johnson

Telcos might be crazy like a fox

The great thing about tracking the telcos is that if you wait long enough, they're guaranteed to pull some really dumb stunts. This week's cases in point: Verizon and BellSouth.

Consumer customers of both companies recently noticed the fine print on their telecom bills that basically said: "We are no longer charging you the Universal Services Fund tax. However, we're replacing it with our own mysterious surcharge, so you won't be seeing any savings."

Talk about a tactic that ticks off customers! This move generated some major responses, including the creation of a Web site named (appropriately enough) Stop the DSL Rip-off (see www.nwdocfinder.com/5148). It also merited a mention in The Onion, a satirical online magazine (see www.nwdocfinder.com/5149).

The upshot? Under pressure from the FCC and consumer groups, the companies late last month removed the mystery charges from consumer phone bills.

Now, here's the thing. Are the telcos just plain dumb? Or are they dumb like the proverbial rabbit that begged not to be thrown into the briar patch? At first blush, telling your customers to their faces that you're ripping them off would seem forehead-slapping stupid.

Consider the endgame, however: It's in the telcos' best interests to keep telecom a highly regulated industry. Judging from the results, they're succeeding: A great way to stay regulated is to incite your customers to call for it.

Why would the telcos want regulation, you ask? Think about it: Regulation ultimately benefits the parties with the most expensive lawyers and lobbyists. Guess what? That ain't Joe and Jane consumer. Telcos have had decades of experience tweaking and tuning regulations to their favor. They thrive under regulation. If you doubt me, compare their profit margins before and after deregulation. No matter what you think of the Telecommunications Act of 1996, one thing it did for sure was cut into telecom margins.

It's Economics 101: In a competitive market, regulation leads to stagnation and fat margins for the regulated entity. Deregulation leads to competition, which results in lower fees and better service.

That's why I'm pushing back on folks who keep insisting the solution to moves like Verizon's and BellSouth's is to increase regulation. A representative for the Stop the DSL Rip-off site wrote me to say, "It is time for consumers to speak up and demand FCC action!"

With all due respect: No, it's not. It's time for consumers to decide to stop doing business with companies that rip them off.

A decade ago, one might have been able to make the argument that the telcos were the only game in town for communications services. Now that's no longer true. In Verizon's territory, Comcast is saturating the airwaves with ads encouraging folks to switch to its new triple-play services. (My favorite: Two attractive young women are discussing a cute guy. One says to the other, "But did you hear? He uses Verizon." Both make disgusted faces.) And the satellite companies are serving folks in the boonies.

Competition is a wonderful thing. We should support it. Leave regulation to the lawyers.

Johnson is president and chief research officer at Nemertes Research, an independent technology research firm. She can be reached at johna@nemertes.com.

HP desktops to use Intel's vPro bundle

BY BEN AMES, IDG NEWS SERVICE

HP is using streamlined IT management as a sales pitch for its latest line of PCs, including the first desktops to use Intel's vPro technology.

A computer running the vPro bundle uses software and hardware — including Intel's new Conroe Core 2 Duo processor — to automate some aspects of IT management and network security. Intel formally announced the platform last week, as Gateway and Lenovo Group also start selling vPro-enabled desktops.

Only the desktops offer the vPro option, while the other new PCs take advantage of the flurry of chips launched in recent months, including Intel's Merom Core 2 Duo for the notebooks and a choice of Intel's Woodcrest Xeon 5100 or Advanced Micro Devices' (AMD) Rev. F Next-Generation Opteron for the workstation.

HP promised to make life easier for the IT managers who maintain these machines by preloading its OpenView Configuration Management agent on all commercial notebooks, desktops and workstations. That product has been an option in the past.

OpenView will bolster Intel's Active Management Technology, an ingredient of vPro, allowing IT managers to boot and repair PCs remotely, says John Snaider, HP's vice president for desktop PCs.

Other enhancements on the desktops include Trusted Platform Model (TPM) 1.2 security chips, a second hard drive for real-time data backup and a virtual partition on the hard drive for encrypting sensitive data, says Brian Schmitz, director of desktop product marketing for HP.

HP is selling the dc7700 desktop for $643, plus a premium for the vPro option. The company plans to launch the dc5700 and dc5750, which will be available with either Intel or AMD chips, in the fourth quarter.

HP plans to ship the xw9400 workstation later this month for $1,800. The notebooks include the HP Compaq 9400 for $1,300; 8400 for $1,550; nx7400 for $849; nc6400 for $1,200; 6300 for $799; and 4400 for $1,479. ■

RightNow upgrades CRM suite

BY ANN BEDNARZ

RightNow Technologies this week is expected to unveil the latest version of its hosted CRM suite, which features a revamped client architecture, new software for soliciting customer feedback, and enhanced analytic and reporting capabilities.

RightNow 8, which is due to be available in December, is aimed at helping companies better manage and improve the quality of their customers' experiences, says Greg Gianforte, president and CEO of the company. It's the result of a two-year, $25 million engineering effort, he says.

Tell us more

The emerging market for feedback management software will grow more than

35%

per year as companies seek to learn more from their customers, employees and partners, predicts research firm Gartner.

New to RightNow's browser-based software — which it delivers via a multitenant hosting model — is a feedback module that lets companies capture customer feedback in real time and take action. For example, a company could route product-related customer comments to design teams, which might then contact customers to solicit more detailed information for future product revisions.

Built-in escalation rules let companies decide how they want negative feedback handled. "If a response is below some minimum that a company establishes, that feedback will go directly to a supervisor in the customer service area, or a manager, or whoever is designated," Gianforte says. "Because it's in real time, the company can take intervening action before the customer becomes bitter and switches to another vendor."

Also new to the suite is a workflow engine with a graphical design tool. The Customer Experience Designer includes prebuilt templates that business users can modify to map such processes as handling a customer complaint or registering a product online. "It's a Visio-like interface that lets you map out the way you want the experience of your customer to be conducted," Gianforte says.

On the analytics front, RightNow 8 bolstered its capabilities with Report Design Center, a tool that lets users assemble tables, charts and fields to create reports and assemble customized analytics dashboards. With historical trending, users can compare current and projected information with historical performance data, such as lead conversion rates and customer satisfaction rankings.

To increase user productivity, RightNow added a workspace design tool that lets administrators customize desktop layouts depending on users' roles — adding or reorganizing fields, tabs and tasks, for example. Packaged templates include sales, marketing and customer service profiles at the executive, manager, sales representative and agent level.

The technology "allows us to start designing custom processes for particular vertical industries," Gianforte says. With RightNow 8, the vendor is introducing its first products tailored for different sectors. Each features built-in industry-specific processes, terminology, workflows and analytic dashboards.

The first versions target government, business-to-business and business-to-consumer environments. Traditional CRM vendors with premises-based software, such as SAP and Oracle, have long offered industry-specific versions of their software. But it's a new approach for vendors that deliver CRM software-as-a-service — a market that includes Salesforce.com and NetSuite.

RightNow has not finalized pricing for RightNow 8. With past versions, a two-year license started at $1,250 per user. ■

BE AT THE DOOR
WAY BEFORE
OPPORTUNITY
KNOCKS.

Caution urged on endpoint VPN security

BY TIM GREENE

Remote access?

Software that determines whether remote machines meet corporate security standards before they access the company VPN can protect networks from malicious outbreaks, but they aren't perfect.

Upside	Downside
Checks for updated virus protection.	Security upgrades can lag far behind discovery of new threats and vulnerabilities.
Allows access only to machines with patched operating systems.	Fixing shortcomings may interrupt business processes, because they take too much time.
Ensures personal firewalls are running and configured properly.	Zero-day attacks are not discovered.
Makes sure registry settings meet security standards.	Machines of business partners — the biggest potential threat — probably cannot be scanned as thoroughly.

Companies consider it important to check whether or not remote computers meet corporate security profiles before they gain VPN access, but endpoint checking cannot address all the problems the machines might cause.

Because endpoint security can prevent infected machines from spreading malicious code to corporate networks via VPN connections, it has become a standard offering of the most remote-access VPN vendors, including Aventail, Check Point, Cisco, Citrix, F5 Networks, Juniper and Nortel.

But the technology also has inherent shortcomings. It cannot guarantee that a particular computer will be free of infection when it joins the network. For instance, a key area for endpoint software is to check for antivirus software, and it relies on periodic updates of signature libraries to be effective.

It takes a certain amount of time for antivirus vendors to discover viruses, identify signatures for them and update their signature libraries. During that interval, the virus could infect a machine that is running the latest version of corporate-prescribed antivirus software. The endpoint check would find the computer in compliance with security requirements and admit it to the network, where it could introduce the virus.

"The problem with endpoint security is that in concept it's a great idea," says Zeus Kerravala, an analyst with the Yankee Group, "but in practice it has problems."

Shortcomings

At the recent Black Hat Security Conference, this type of endpoint security was called a shortcoming at a controversial session that poked holes in network access control (NAC) schemes. "It all breaks down to what is being checked, and is the information helpful or not?" says Ofir Arking, CTO of NAC vendor Insightix, who delivered the talk.

Much of the problem lies with how fast businesses can update the client software as new vulnerabilities, exploits and malware are discovered, he says. For example, when a flaw is found in an operating system that leaves it vulnerable to attacks, patches are issued, but in many cases are not installed immediately.

The time it takes to issue the patches and checking whether the patches break other applications on corporate computers delay installing them, Arkin says. The business also has to schedule time to install the patch and roll it out to all of the computers it maintains, further delaying when the operating system is made safe.

The business can update its endpoint-checking software to seek the patch as part of the security check it runs on endpoints. This process can take weeks or months, Arkin says.

Regardless of how quickly virus updates or patches are issued, new attacks cannot be prevented using endpoint checkers, Arkin says.

He points out that beyond the difficulties of keeping remote-machine software up-to-date, endpoint checking doesn't ensure unauthorized users are kept off the network or that sensitive information isn't transferred over VPN links.

Separately from the security concerns, endpoint checking can interfere with user productivity, Yankee Group's Kerravala says. Many endpoint security checkers can divert noncompliant machines to what is known as a remediation site, where the software needed — including virus signature update, operating system patch or personal firewall — can be downloaded. It sounds good on paper, but it has a major flaw. "It interrupts the workflow," he says.

He paints the scenario of a salesperson about to enter a meeting who tries to log on to the VPN to download the latest version of a presentation, only to be denied access because the operating system on the computer needs a patch. Even if the endpoint-checking software redirects the machine to a remediation site, the time it takes to download and install the patch is likely to delay seriously the delivery of the presentation.

This can keep VPN administrators from using endpoint checkers, Kerravala says. "The last thing you want to be is the thing that interrupts workflow," he says.

It is possible to issue one-time exemptions so users, such as the salesperson who needs the presentation, can reach the VPN without passing the endpoint check, he notes. But if the problem arises repeatedly and continues to block important work, the exemption can replace the rule. "It becomes the every-time exemption," he says.

Mitigating problems

Education of users to update their computers routinely can mitigate the problem, but enforcement becomes a problem. "Are you going to fire your top sales guy because his virus signatures aren't updated?" Kerravala asks.

Some security vendors check endpoints before allowing remote computers to join VPNs, and if a check determines that the machine cannot pass inspection it may be allowed limited access. Check Point's Integrity software performs this task and can, for example, let a guest computer that cannot be scanned access the Internet but not gain access to any other network resources.

Other vendors say their products keep track of what endpoints are up to and block them if they engage in malicious activity. Promisec, for example, makes software that requires no client software but blocks harmful processes on the network.

Cisco, as part of its Security Agent software, analyzes behavior to protect networks from malicious behavior by endpoints. This type of host intrusion prevention that looks for inappropriate activity rather than appropriate configuration is also offered by ForeScout Technologies, MetaInfo, Privacyware and Sana Security.

VPN protection using endpoint checking is most effective for the machines that are most likely to be trustworthy — those owned by the corporation, says Joel Snyder, senior partner in technology consulting firm Opus One and a member of *Network World's* Clear Choice Alliance. That is because those owned devices can readily be equipped with endpoint-scanning agents.

But VPNs, particularly SSL VPNs, are frequently used to grant access to business partners that are unlikely to allow such scans, the devices that represent the biggest threat. "Endpoint security checks work only when you need them least," Snyder says.

Cisco, Juniper and Microsoft have NAC schemes that incorporate endpoint checking as part of a larger architecture that determines safety of devices and enforces whether they gain access. The downside is that these architectures could take another 18 months until the software and hardware needed to implement them are ready, Kerravala says.

The bottom line is that endpoint security as it exists in VPN products is inadequate to block all the potential threats a remote computer represents to a corporate network. But it does have value, especially if it is a cog in a larger effort to protect the network, Snyder says.

"Endpoint checking won't ultimately be in the VPN box," Snyder predicted earlier this year. "It will be in a NAC box. There will be just a thin layer of endpoint checking in the VPN gateway that punts off to policies that are defined on a different box." ■

nww.com

VPN security

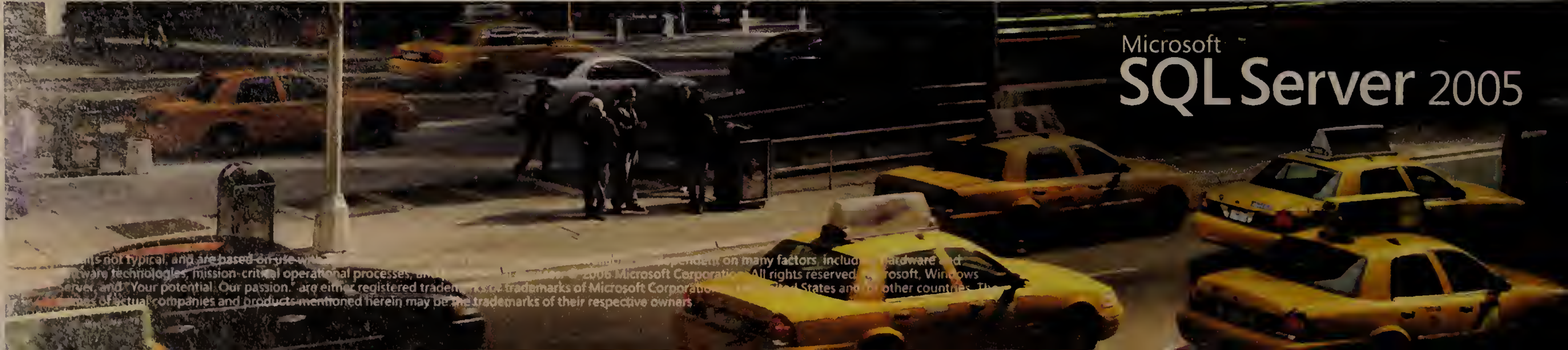
Read the latest about VPN security in *Network World's* newsletter on that subject.

www.nwdocfinder.com/5147

CONCIERGE

A Stock Market Processing 300 Million Transactions a Day. Running on Microsoft SQL Server 2005.

NASDAQ, the largest U.S. electronic stock market, lists companies from 37 countries. Their crucial trading and messaging systems use SQL Server™ 2005 to handle up to 64,000 transactions per second with 99.999% uptime.* See how at **microsoft.com/bigdata**



[illegible]lts not typical, and are based on use w[illegible] dependent on many factors, includ[illegible] hardware and [illegible]ware technologies, mission-critical operational processes, an[illegible] © 2006 Microsoft Corporation. All rights reserved. [illegible]rosoft, Windows Server, and "Your potential. Our passion." are either registered tradem[illegible] trademarks of Microsoft Corporation [illegible] States and/or other countries. The [illegible] of actual companies and products mentioned herein may be the trademarks of their respective owners.

TECHNOLOGY UPDATE

■ AN INSIDE LOOK AT TECHNOLOGIES AND STANDARDS

Content compression accelerates apps

BY HOOMAN BEHESHTI

In Web applications, client response time and latency represent challenges for network and systems administrators. Content compression is one of the most popular methods used to get content from the application to the client faster.

For applications that serve a global community of users where there is no control over the client network, compression is most often deployed in an asymmetric appliance that sits in front of the Web application. Sometimes known as application front ends, these appliances provide compression along with a number of other features, such as TCP acceleration/ offload, load balancing and SSL offload. Here, asymmetric refers to the the appliance being deployed only at one side of the delivery path (that is, the data center, in front of the Web servers).

A lot of Web content is text based (such as HTML, XML and CSS) and, therefore, highly compressible. Because compressing content reduces the number of bytes that traverse the network from the application to the client, it's a natural step toward reducing response times.

All popular browsers support compression. Through the use of the Accept-Encoding request HTTP header, the client indicates that it can receive compressed content. It also indicates through the same header the compression algorithms it supports, gzip and deflate being the most common. This tells the server side of the application (in this case, the application front end) that the requested content can be compressed before it's sent to this client.

An application front end requests the content from the server, compresses it through one of the compression algorithms supported by the client, inserts the proper HTTP headers to indicate that it's compressed (and the algorithm used) and then sends it to the client. Because the compressed version is smaller than the original, the object will reach the client faster. The client browser decompresses the object and renders it for the user. Even though there is a small amount of overhead for the client in the decompression task, it is negligible when compared with the benefits of significantly reducing the number of bytes that traverse the network.

The compression ratio will vary from file to file and the efficiency of the algorithm being used. Some text files can be compressed by as much 90%, while others can't be compressed much. The appliance should let administrators configure which files are to be compressed and which files aren't. Some browsers (or browser versions) may have problems decompressing some content. The appliance should also allow configuration of detailed exception rules that will indicate which requests not to compress, despite the HTTP request headers.

Reducing content size is the most obvious benefit of content compression in an application front end, but it also reduces outbound bandwidth for an application. In an environment where bandwidth costs are an issue, or if application bandwidth is nearing its allotted limit, content compression provides relief.

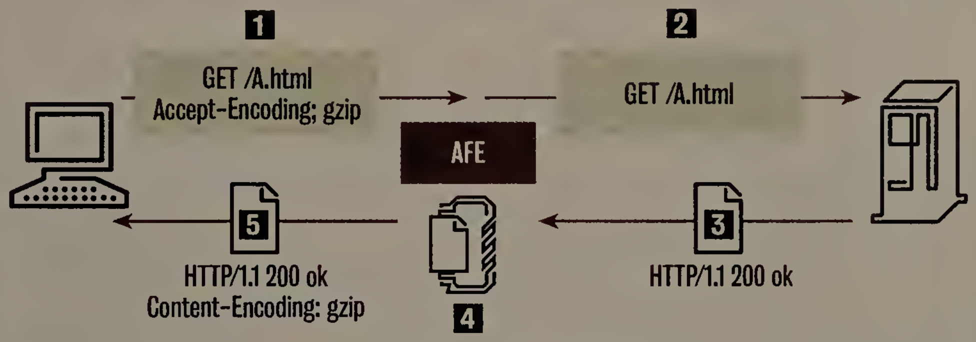
Compression on an application front end can also work as an offload technology to relieve a server from unnecessary overhead related to compression.

These benefits make compression one of the most vital features in application front-end appliances and one of the main reasons the technology is being deployed in an increasing number of application infrastructures.

Beheshti is vice president of Technology for Crescendo Networks. He can be reached at hooman@crescendonetworks.com.

HOW IT WORKS: CONTENT COMPRESSION

Content compression reduces the number of bytes that traverse the network, which reduces response times of Web applications.



1 Client sends request for file to server via application front end (AFE). The Accept-Encoding header indicates that it supports gzip compression.

2 An application front end requests the file from the server on behalf of the client.

3 The server responds with the requested content.

4 The application front end compresses the file.

5 The application front end sends the compressed file back to the client. The Content-Encoding header indicates that the content is compressed via gzip. The client will then decompress it and render it for the user.

Got great ideas?

■ *Network World* is looking for great ideas for future Tech Updates. If you've got one, and want to contribute it to a future issue, contact Senior Managing Editor, Features **Amy Schurr (aschurr@nww.com).**

Ask Dr. Internet

By Steve Blass

I forgot the admin password on my Macintosh OS X system. How can I crack or reset the password?

Mac OS X is based on BSD Unix, so one way to crack Mac passwords is with Unix password-cracking tools. In particular, John the Ripper has a good reputation for being successful in cracking Mac OS X passwords. While this can be useful to systems administrators, it points out that password security can be broken fairly easily.

Even easier than downloading and installing password-cracking software is using a Mac OS installation disk to reset the administrator password. If this is an Xserve server, be sure to unlock the drive lock so you can mount the installation disk. Insert the install disk and click on the "Install Mac OS" icon. Click the Reset button on the installation screen, and it will begin the installation process. Click through screens until you see the normal menu bar menus on your screen. Click on the Utilities menu and choose "Reset Password." Follow the prompts to change the admin password. After resetting the password, choose Quit from the Installer menu. Remove the installation disk from the drive and restart. You should be able to log on as administrator using the new password you just set.

Blass, a network architect at Change@Work in Houston, can be reached at dr.internet@changeatwork.com.

GEARHEAD
INSIDE THE NETWORK MACHINE

Mark Gibbs

Differencing with HTML Match

An interesting question came up on a list we subscribe to: How can you compare two versions of a Web page to see what changes have been made?

This question was raised by someone acting as an expert witness in a case of Web-site plagiarism. Following the obligatory flurry of legal shots, the offender agreed to make changes. Now the problem is determining if changes have been made.

Making a copy of a site isn't hard — the wGet utility (www.nwdocfinder.com/5134) is one of the easiest tools for this. Everyone running a *n*x (that abbreviation covers all *nix versions as well as Linux) should find wGet already installed.

For Windows you'll want to visit the Wget on Windows page (www.nwdocfinder.com/5135) for the Win32 version, and you'll want to acquire the wGetGUI front end for wGet (www.nwdocfinder.com/5136), which gives you a GUI that helps you run wGet using a batch file it creates.

So, getting a copy of the Web content is easy, and to do the comparison or differencing of a recent version of the site and a previous one, most *n*x people would use the diff utility (www.nwdocfinder.com/5137), while Windows users might use Microsoft's File Compare utility or the newer WinDiff.

WinDiff comes as part of the Windows XP Service Pack 2 Support Tools (www.nwdocfinder.com/5138), or if you don't want to install the Windows Genuine Advantage plug-in (a prerequisite for downloading and perhaps the dumbest antipiracy scheme so far), you can download WinDiff from Keith Devens' site (www.nwdocfinder.com/5139).

WinDiff is reasonably good, but not great, at showing how the two input files differ and provides a few options for what information is displayed about changes. Oddly, on our Windows XP Professional SP2 computer, the tool seems to have some fairly serious GUI maintenance problems, such as not completely redrawing the display. But what WinDiff doesn't do is make it easy to deal with the fact that the offending Web site was edited with Microsoft FrontPage.

What is needed is a differencing tool that can filter the inputs in useful ways.

FrontPage and other editing programs add their own markup with wild abandon, so although you can see which content has been changed, figuring out whether the changes lie solely in the markup can be difficult. What is needed is a differencing tool that can filter the inputs in useful ways.

HTML Match (www.htmlmatch.com), from Salty Brine Software, is designed for exactly this kind of work. Salty Brine also publishes FreeDiff (www.freediff.com), a simpler (and free) differencing tool.

HTML Match lets you compare original and revised content from locally accessible files or from URLs (the program downloads the content to a temporary local file). You also can compare local files with URL-derived content, and you can select to see just the visual differences, the underlying source code or the embedded text content. Finally, you can see the differences, shown at character, word or line levels of detail.

You also can choose whether text extraction should be done by HMTL Match's built-in text-extraction engine, followed by Microsoft Word (if that is installed) if the internal engine fails — or vice versa, to make sure that if the content is hard to analyze, you stand a chance of getting at whatever text might exist. There also are options —such as ignore white space and ignore case — to filter the content further.

The displays are color-coded to highlight the differences, and you can set bookmarks (these disappear when the files are closed), jump to an editor to modify the files, and print the analysis for either or both files showing all lines, just the differing lines or just the identical lines. You also can run the program using command-line arguments, and have the option to save the results in an HTML file (normal operation doesn't support saving the differences report in a file).

There are many tools for differencing, but of all we've looked at, HTML Match is the best. At $27.95 it is a steal.

Do you know the difference? Tell gearhead@gibbs.com.

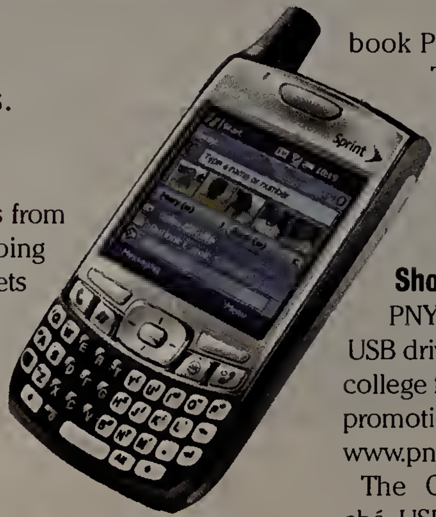
CoolTools

Quick takes on high-tech toys.

Keith Shaw

Last week's holiday and early deadlines from our taskmasters prevented me from doing some testing this week — so let's look at some new gadgets coming down the pike:

Palm launches Treo 700wx with Sprint



The Treo 700wx has a Windows operating system on a Palm device on the Sprint network.

The latest smart phone from Palm is the Treo 700wx, which runs Windows Mobile 5.0 Pocket PC Phone Edition software and accesses Sprint's Palm evolution data optimized (EV-DO) wide-area wireless network. The device is available at Sprint stores and business channels for $500 (after discounts and promotions). The 700wx is the first Windows Mobile-based Treo smart phone for Sprint, which also sells the Palm OS-based Treo 700p (the Treo 700w is available on the Verizon Wireless network).

The 700wx includes the Windows Mobile Messaging and Security Feature Pack, which has Direct Push technology, native Secure Multipurpose Internet Mail Extension support, certificate-based authentication for all Exchange data, and remote and local device-memory wiping, Palm says. The 700wx offers access to Good Technology's Good Mobile Messaging application for over-the-air provisioning, and real-time access to push-based e-mail, calendar, contacts, notes and tasks. The system supports the Good Mobile Defense application and Good Mobile Intranet (connecting users to such Web-enabled enterprise applications as salesforce automation and CRM applications).

The 700wx has built-in dial-up networking, which lets users take advantage of Sprint EV-DO network access by using the 700wx as a modem between a notebook PC and the network.

The device includes such hardware features as a 1.3-megapixel digital camera, 64MB of RAM for additional applications, Bluetooth 1.2 wireless, a removable battery, memory card expansion slot that supports Secure Digital (SD), SDIO and MultiMediaCard cards), and a 240-by-240-pixel transflective screen.

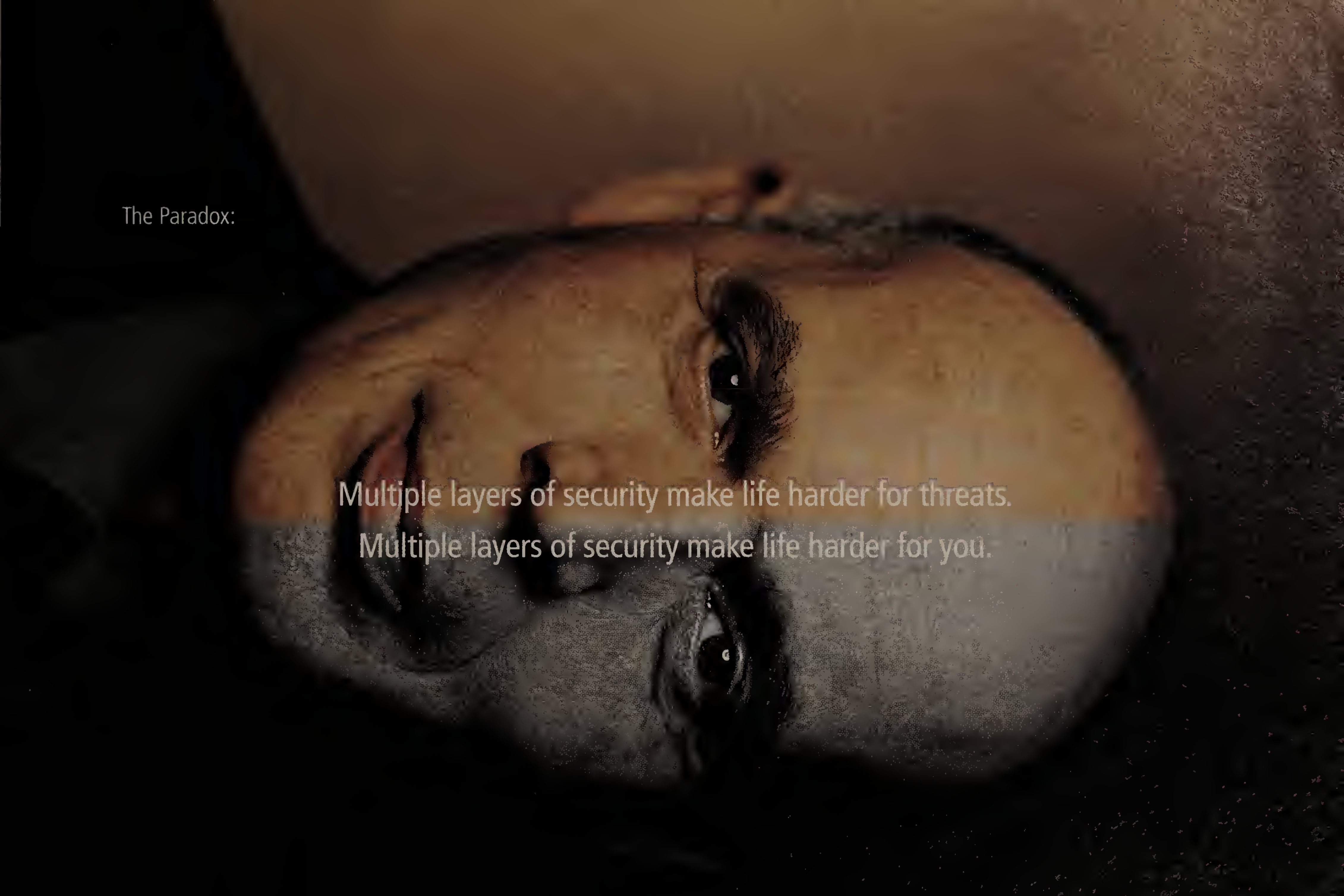
Show school spirit on your USB drive

PNY Technologies is running a promotion from now until Sept. 22 –– a 512MB USB drive for $14.99 and a 1GB drive for $29.99, which includes a preseason top-25 college football team logo. To get the promotional price, head to www.pny.com/top25.

The Collegiate Attaché USB 2.0 flash drive has more than 150 fully licensed USB drives with other college, university and athletic logos, so if your alma mater isn't good enough to be in the top 25 football teams (ahem, Syracuse Orangemen), you can still buy a 512MB drive for $19.99.

A 1GB USB drive for $30? Makes you want to buy one even if you didn't go to college.

Why just read this when you can see and hear Keith online? There's a new Cool Tools video every Thursday, and the Twisted Pair podcast debuts every Friday at www.networkworld.com. Shaw can be reached at kshaw@nww.com.


The Paradox:
Multiple layers of security make life harder for threats.
Multiple layers of security make life harder for you.

The Answer: Proven security.

- Anti-Spam & Anti-Spyware
- Network Access Control
- Intrusion Prevention
- Desktop Firewall
- E-Mail Security
- Anti-Virus

Security threats are mounting in number—and they're evolving in complexity. Your security must evolve as well. This used to mean managing multiple products without integration, which created operational challenges, risk, and increasing costs. Not any more. With McAfee® Total Protection for Enterprise, you'll have comprehensive, integrated protection. You'll control everything—from anti-virus to network access control to anti-spyware—all from a single management console. McAfee Total Protection solutions are engineered to provide maximum manageability and deliver total endpoint security without compromise. McAfee, the dedicated security company that blocked or contained 100% of the top attacks in 2005, delivers proven results backed by more than 15 years of experience. Secure your business advantage. Learn more at www.mcafee.com/total

Proven Security™

On Technology
John Dix

Security is SOP for business

At last week's Security Standard conference in Boston — which was hosted by *Network World* and other IDG publications — speakers talked as much about the business of security as the technical options and details.

All agreed that security is now standard fare in boardroom discussions. "Board involvement has changed dramatically," said John Schramm, senior vice president of enterprise information security for Fidelity Investments and a panelist in one session.

"They want to know about the biggest risks, what we are doing about them and how they can help," he said.

It's no wonder, agreed panelist Tom Bowers, manager of information security operations with a Fortune 100 pharmaceutical company that didn't want to be identified. Security breaches have put some companies out of business and deflated the stock value of others by 20% to 40%.

"Up until a few years ago security was reactionary," said panelist Scott Blake, CISO for Liberty Mutual Insurance Group. "Something bad would happen to a company, and it would decide it couldn't allow that to happen again so would spend some money. Now we're all trying to get out ahead of things by making investments."

How do you justify the investments? Many speakers at the event were down on using ROI.

ROI works for things like antivirus tools, Bowers said, but you have to know the value of what is at risk and be able to measure that: "We have PDAs all over the world with corporate information on them. What is the value of that information and what is the risk?"

That sentiment was echoed in another session featuring Lawrence Kinsella, CFO for BT Global Financial Services, which operates a managed extranet for financial firms. "We don't do true ROI analysis on security. The most important thing to a company like ours is our reputation. You can't put a value on that," he said.

Kinsella shared the podium with his company's CSO, Lloyd Hession, who said you can either accept risk, mitigate it or assign it to someone else, but you will always face risk-reward trade-offs.

Issuing a router patch to 20,000 devices, for example, could be riskier than not patching, if the vulnerability has yet to be exploited in the wild.

Speaking of patching, Ryan Hamlin, general manager of Microsoft's Technology Care and Safety Group, told the conference crowd in another panel discussion that Patch Tuesday won't go away with the arrival of Vista. "Software is complicated," he said. "But hopefully, the frequency of the patches, the urgency of patching goes down."

—John Dix
Editor in chief
jdix@nww.com

Opinions

Views on Vista

"Vista testers fuming as beta judged lacking" (www.nwdocfinder.com/5063) states that no antivirus products currently work on Vista Beta 2. Using the public beta, I have installed a beta of Trend Micro's PC-cillin, CA's antivirus and (after applying the latest Beta 2 patches) AVG's free antivirus product. Also, Beta 2 has been fairly stable on the PCs I have put it on.

Edward Baichtal
IT manager
AirLink Communications
Hayward, Calif.

Regarding "Vista testers fuming as beta judged lacking": Microsoft doesn't need a home run; the financial analysts need a home run. With as much of the market as Microsoft has locked up, there is no non-Windows OS for people to migrate to en masse, and they're not going to drop XP just because the new version of Vista is screwed up. For years Microsoft's biggest weakness in terms of its public perception has been that it makes buggy code. If Microsoft took the time and got it right, it could wait years before putting out a new operating system. I still use Windows 2000, the cleanest release ever. I have yet to see a compelling reason to go to XP. It will be a long time before I go to Vista or recommend it to my clients.

Ray Tracy
Owner
Navion Medical Imaging
Prince George, B.C.

Linux plays nice

Your story, "Linux event shows move to mainstream" (www.nwdocfinder.com/5064) states, "Besides keeping open source systems safe, another issue on the minds of users is making Linux play well with others." In many cases it's not Linux that isn't playing well; it's other systems, which use undocumented, proprietary formats instead of fully documented open standards that are freely accessible to everyone. The most notable example of this is Microsoft, which regularly embraces, extends and extinguishes once-open formats or specifications to be almost open, yet with a tiny tweak to make them not quite interoperable with the open standard and using as many proprietary specifications as possible.

Linux, on the other hand, is trying to interoperate well with proprietary standards or formats: .doc format support in OpenOffice, arguably even better than different Microsoft Office versions; pretty good Win32 application compatibility via Wine; Samba for Windows Networking support; and NTFS support for NTFS Windows file system access compatibility. All of these had to be almost entirely reverse engineered because of incorrect or missing documentation.

Andreas Mohr
Karlsruhe, Germany

Processor still needed

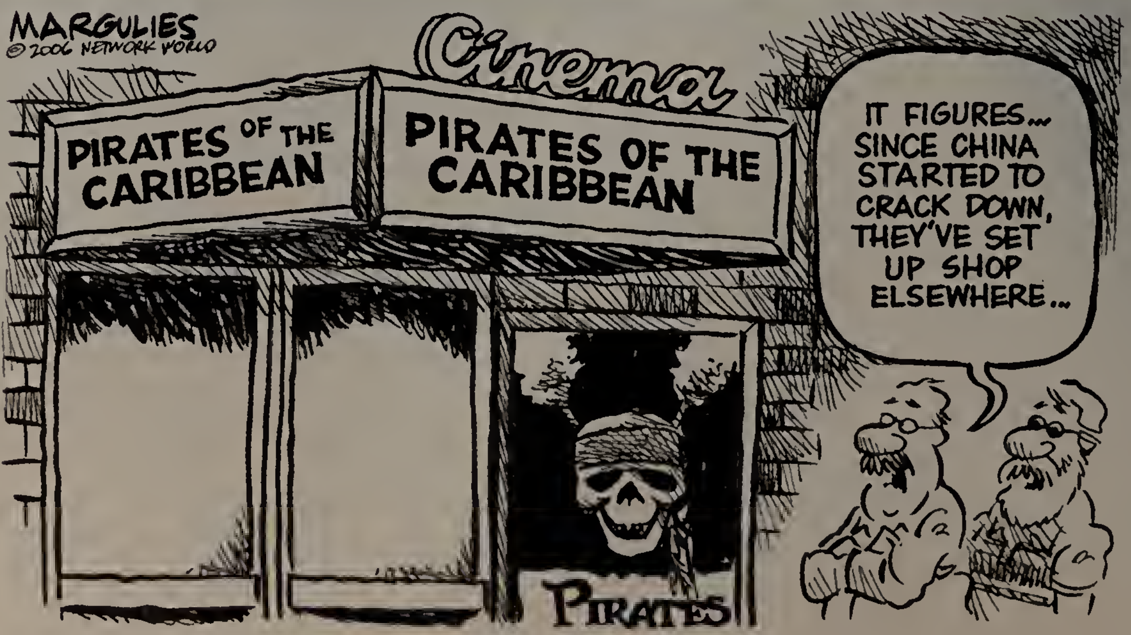
Regarding your Cool Tools item, "USB flash drives evolve into application powerhouses" (www.nwdocfinder.com/5065): Hang on to your laptop for a while yet. A USB drive contains no processor and cannot run anything.

The USB "drives" have improved in speed and capacity enough that they can almost be effectively used as a substitute for a hard drive or CD. You still need a powerful processor, lots of high-speed RAM and someplace to swap that RAM to run modern applications.

Tyson Vickers
Toronto

E-mail letters to jdix@nww.com or send them to John Dix, editor in chief, Network World, 118 Turnpike Road, Southborough, MA 01772. Please include phone number and address for verification.

nww.com **Readers respond**
Find out what readers are saying about these and other topics. **DocFinder: 1030**



CYBER SPACES

Daniel Blum

Accountability is best recipe for compliance

Compare the confusion of implementing regulations, such as the Sarbanes-Oxley Act, with the clear results of breach disclosure accountability legislation, such as California Senate Bill 13. AOL, with its recent search data debacle (see www.nwdocfinder.com/5062), is the latest organization to have its data breach paraded across front-page headlines. Before AOL came the Department of Veterans Affairs and CardSystems.

AOL's desire to share search information with researchers was well intentioned but unsound. Personal information for some users was disclosed and many others may be at risk. A CTO and two other AOL staff members resigned or were forced to leave. While parent company Time Warner's stock registered barely a blip in this case, the career-limiting possibilities of any privacy breach are apparent to IT managers everywhere.

The VA went through a harrowing period while a nation feared those who had worked, fought and sacrificed for it would be subjected to identity theft or worse. In the end, the VA could offer plausible assurances that the data, though stolen, was never compromised. Yet as a result of disclosure and accountability, policies are changing to prevent sensitive data from wandering away in laptops to suburban neighborhoods.

CardSystems was forced to disclose a massive breach of credit card data caused not only by failure to comply with security policy but also by violation of contract governing the use of the data. CardSystems became a corporate pariah, fell into bankruptcy and died. Executives around the world took notice.

Breach disclosure focuses on accountability for results, not the audit process. When data protection joins sales and profit as part of a balanced scorecard for corporate objectives, executives have incentives to reduce risk.

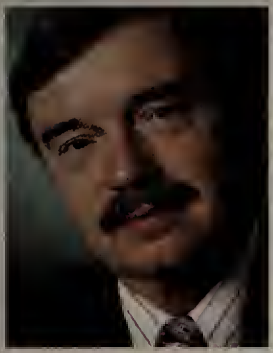
The threat of having to disclose information security failures can . . . encourage proactive change.

On the other hand, SOX — with its stentorian demands for auditor certifications — has produced mixed results. The annual audit has become a security theater of IT practitioners and auditors poring through prescriptive checklists and documents. One can find silver linings of risk management and process automation in SOX, but only after peeling away reams of documentation and audits.

There are useful lessons from these experiences for public policy and internal security programs. The threat of having to disclose information security failures can pose enough reputation risk and legal jeopardy to encourage proactive change.

Yet information is stored or used in many places, with many changing tools and approaches for protecting it. Should we restrict all data to one central server and force all users to physically come to that data center? Or distribute the information widely but only in encrypted form? No planner or auditor can fully prescribe what to do. Responsibility for security needs to be distributed, even within an organization. Create clarity in accountability at each level of business hierarchy, from C-level executives, to business unit managers, to managers of application development or IT infrastructure. Accountability scales; prescriptions do not.

Blum is senior vice president and research director with Burton Group, an integrated research, consulting and advisory service. He can be reached at danjblum@yahoo.com.



REALITY CHECK

Thomas Nolle

Can FMC unite the diverse carrier drivers?

The RBOCs' profit reports for the last quarter show some common trends in their revenues: legacy services and public switched telephone network lines are down, while mobile wireless and consumer broadband are up. Having two market areas up and only one down isn't bad, but if the RBOCs have to invest big bucks in both wireless and consumer broadband, it could crimp their profits. If they have to make a choice, some of our assumptions about the future will not come true. But maybe they don't have to choose — and maybe they can't.

Many in the network industry see fixed-mobile convergence (FMC) as a subset of the overall convergence theme — putting voice on the Internet. Others think IP Multimedia Subsystem (IMS), a technology that can support FMC, is what FMC is about. Both are wrong; FMC is about money — saving it and making it.

FMC's money-saving mission is linked to the propping up of wireline revenues by linking wireline VoIP to wireless. Few players can offer both, so the competition that could reduce VoIP pricing to near-zero levels is sharply reduced. But the amount of infrastructure required for voice convergence like this is peanuts in an RBOC capital budget of billions and does nothing to converge spending from the fixed and mobile sides.

For that, video may be needed. While many think of video as being delivered to the home TV, the new-age IP video has done better delivered to mobile phones or portable appliances. Part of the reason is because the smaller screen size makes bandwidth requirements lower and the low-quality images pose less copyright risk, but also because at-home video behavior is locked in by habit. If you want to sell them something new, you have to grab them on the move.

A dual-mode handset that speaks Wi-Fi at home and 3G on the road is ideal for this. Such a device lets users sample video in the home without airtime charges and take it on the road when they are ready. One person I talked to recently said he was a cellular video prospect every time his child's soccer game coincided with the local ballgame, but these coincidences won't pay for a lot of service. If the handset could be used in the home, yard or for other video uses, it would be easier to get the soccer dad to take it to a game and time-share between the Red Sox and the Matawan Soccer Eagles.

FMC is about money — saving it and making it.

This kind of new video experience would go a long way toward opening doors for the RBOCs. There is no regulatory barrier to this kind of video, no franchising. The revenue stream it creates is separate from that of standard IPTV, so it wouldn't impact a drive to offer traditional home video. It creates an incremental market for video, not a tap on the cable or satellite market, so it dodges competition and builds overall revenue.

Most significantly, this would subsidize the process of creating a new converged network to deliver video flexibly to both the home via DSL and Wi-Fi, and the road via 3G. The cost of technologies such as IMS could be recovered faster from this kind of video convergence than from voice convergence, and video backhaul for cellular sites is a larger issue than backhaul of voice, which we're already doing fairly well.

A focus on video doesn't mean that voice convergence will be ignored. The fact that the cable guys are offering voice services means the RBOCs eventually would have to respond, and FMC voice features such as call handoff to DSL while in the home are valuable to users. However, they sap revenue for the RBOC, which would otherwise sell more mobile minutes to these users. What would be a positive is that FMC voice might induce more users to use mobile phones by letting a wireless home phone become a standard cell phone outside the home.

Video and broadband have always represented the opportunity choice for improved profitability, and FMC the cost management choice. A focus on video services in FMC applications would let providers make an opportunity out of both.

Nolle is president of CIMI Corp., a technology assessment firm in Voorhees, N.J. He can be reached at (856) 753-0004 or tnolle @cimicorp.com.

IPS: Slow down for safety

Tests show high performance doesn't always mean high security.

BY DAVID NEWMAN, NETWORK WORLD LAB ALLIANCE

High-end intrusion-prevention systems move traffic at multigigabit rates and keep exploits out of the enterprise. The problem is they might not do both at the same time.

In lab tests of top-of-the-line IPSs from six vendors — Ambiron TrustWave (formerly Lucid Security); Demarc Threat Protection Solutions; Fortinet; NFR Security; TippingPoint, a 3Com company; and Top Layer Networks — we encountered numerous trade-offs between performance and security.

Several devices we tested offered line-rate throughput and impressively low latency, but also leaked exploit traffic at these high rates. With other devices, we saw rates drop to zero as IPSs struggled to fend off attacks.

In our initial round of testing, all IPSs missed at least one variant of an exploit we expected they'd easily catch — one that causes vulnerable Cisco routers and switches to reboot. While most vendors plugged the hole by our second or third rounds of testing (and 3Com's TippingPoint 5000E spotted all but the most obscure version the first time out), we were surprised that so many vendors missed this simple, well-publicized and potentially devastating attack (see Can anyone stop this exploit?, page 46).

These issues make it difficult to pick a winner this time around (see NetResults, page 42). If high performance is the most important criterion in choosing an IPS, the TippingPoint 5000E and Top Layer Networks' IPS 5500 are the clear leaders. They were the fastest boxes on the test bed, posting throughput and latency results more commonly seen in Ethernet switches than in IPSs.

Of course, performance isn't the only criterion for these products. The 5000E leaked a small amount of exploit traffic, not only in initial tests but also in two subsequent retests. TippingPoint issued a patch for this behavior two weeks ago. The 5000E also disabled logging in some tests. That's not necessarily a bad thing (indeed, TippingPoint says customers prefer a no-logging option to a complete shutdown), but other devices in the same test kept logging at slower rates.

The IPS 5500 scored well in tests involving TCP traffic, but it too leaked small amounts of exploit traffic. Top Layer attributed this to its having misconfigured the firewall policy for this test.

IPSs from Demarc and NFR Security use sensor hardware from the same third-party supplier, Bivio Networks. The relatively modest performance results from both IPSs in some tests might be caused by configuration settings on the sensor hardware — something both vendors discovered only after we'd wrapped up testing. On the plus side, both IPSs stopped all attacks in our final round of testing.

Ambiron TrustWave and Demarc built their ipAngel-2500 and Sentarus IPS software around the open source Snort engine. The performance differences between them can be attributed to software and driver decisions made by the respective vendors.

Fortinet's FortiGate-3600 posted decent results in baseline tests involving benign traffic only, but forwarding rates fell and response times rose as we ratcheted up attack rates.

We should note that this is a test of IPS performance, not security. This is a test of IPS performance, not security. We didn't measure how many different exploits an IPS can repel, or how well. And we're not implying that just because an IPS is fast, it's secure.

Even so, security issues kept cropping up. As noted, no device passed initial testing without missing at least one exploit, disabling logging and/or going into a "fail open" mode where all traffic (good and bad) gets forwarded.

This has serious implications for IPSs on production networks. Retesting isn't possible in the real world; attackers

See IPS, page 42

IPS usability is a mixed bag

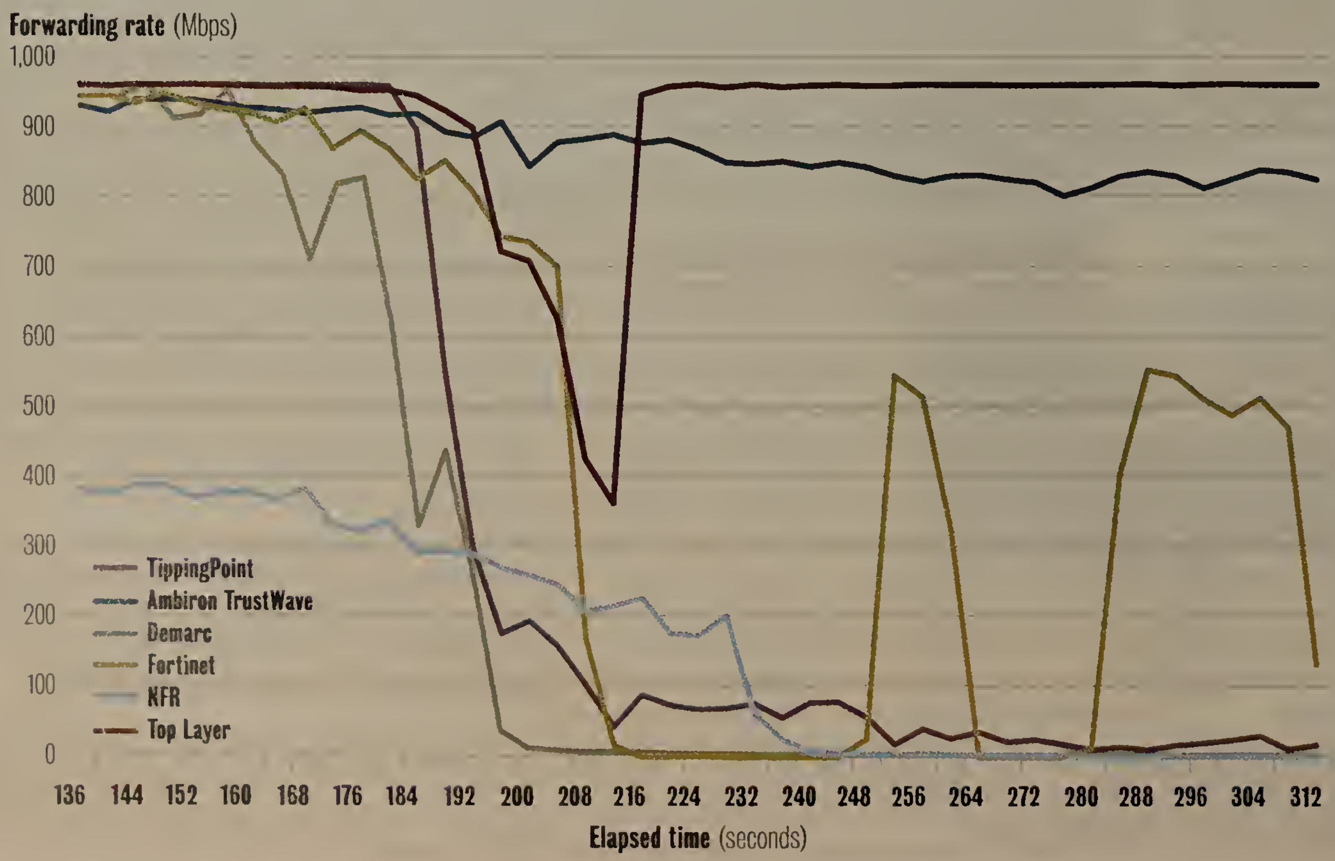
The most important feature of an intrusion-prevention system is whether it does the job you bought it for. That said, it also needs to be usable, in the sense that it supports the network manager in the day-to-day tasks that go hand in hand with using an IPS in an enterprise setting. After shaking out the IPS products for performance, we took them back into the test lab to look at them from another angle entirely: usability.

The clear winner in terms of usability was 3Com TippingPoint's Security Management System used to drive the TippingPoint 5000E, a product that turned in above-average performance on every task we set. Honorable mentions go to NFR Security's Sentivist Management Platform used to control its Sentivist boxes and Top Layer Networks' IPS 5500, which are products anyone trying to manage an IPS would find meet their needs easily, with a minimum of wasted effort.

For the full results of this usability testing, go to www.nwdocfinder.com/5124.

TCP forwarding rates under attack over time

Average forwarding rates as we report in our main performance results charts are useful for comparing baseline and attack results, but they don't tell the whole story. For most IPSs, TCP forwarding rates degrade over time as they fend off attacks. This graphic shows the results over time when exploit traffic comprised 16 percent of the total load — the heaviest attack we used.



LGB
10/10/06
Hyatt Regency
Long Beach, CA

SEA
10/12/06
Westin Seattle
Seattle, WA

STL
10/17/06
Hyatt Regency
Saint Louis, MO

NYC
10/19/06
Hilton New York
New York, NY

NETWORKWORLD LIVE Technology Tour

Network & Application Acceleration

Shifting to a Higher Gear

"Faster!"—even if the apps are inefficient.

"Faster!"—even if the architecture is weak.

"FASTER!!"—even if the support is missing.

In the drive for better performance, greater efficiency, and better ROIs, there's just one demand, no excuses, and dozens of questions you need to answered fast:

- Is it better to implement in-house solutions? Or trust outside managed-service providers?
- Deploy dedicated, single-benefit appliances? Or build flexible, enterprise-wide platforms?
- Be lean, technically-efficient, and centrally-driven? Or scalable, management-transparent, and user-accessible?
- Sacrifice a little security for a lot of speed? Or sacrifice guaranteed profits for uncertain protection?

The fastest way to arrive at a solution? Attend **Network & Application Acceleration: Shifting to a Higher Gear** the new Network World LIVE Technology Tour event coming in October. Let industry expert Jim Metzler accelerate your understanding of the truths and tradeoffs of:

Server Consolidation · Compression · Caching · Differencing · Read Ahead · TCP acceleration · Route Control · QoS · MPLS · SSL Offload · Load Balancing · Wide-Area File Systems (WAFS)

This is the kind of inside, fast-lane knowledge you need in today's world of network and application acceleration. And the only way to this expertise free is to reserve a seat for at this event for yourself. After all, your enterprise's need for speed is relentless. And thanks to Network World, there's no excuse for falling behind!

Who should attend?

> Network and IT Managers
> Network and IT DIrectors
> Directors of Operations
> CIO's and CTO's

Event Host:

Dr. Jim Metzler
President,
Ashton, Metzler and Associates

Platinum Sponsors:

Akamai · CITRIX · EXPAND networks · Juniper NETWORKS · PACKETEER · riverbed

Gold Sponsors:

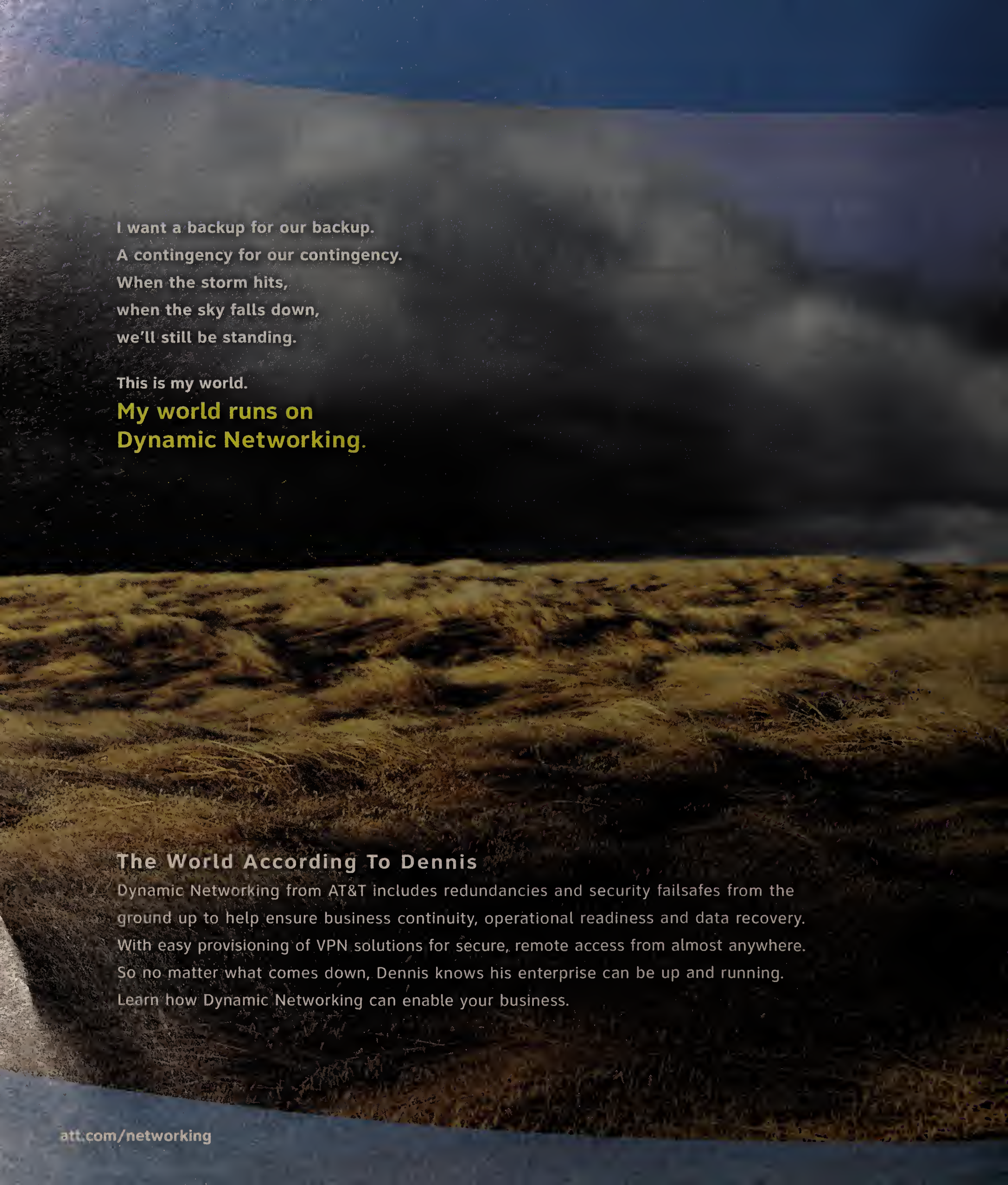
ipanema Technologies · NETLI · Network Physics · Silver Peak

Top 10 Takeaways

1. **SAME DIFFERENCE:** a comparison of leading acceleration techniques
2. **BRAND X:** a solution-driven review of top acceleration products
3. **INSIDE-OUT:** pros and cons of in-house management vs. managed service providers
4. **STRATEGY-TACTICS:** focus on individual problems or plan for any eventuality?—the answer
5. **SURGICAL SKILLS:** how to work the OSI model for maximum through-put
6. **CRYSTAL CLEAR:** the management case for transparent solutions
7. **NOT SO FAST:** the limits of a scalable solution
8. **SLL-OUT:** how acceleration impacts security
9. **SLICK:** factors that enhance the performance of acceleration products
10. **SMOOTH:** the new PoV on QoS

NETWORK & APPLICATION ACCELERATION | QUALIFY TO ATTEND FOR FREE | REGISTER AT

www.networkworld.com/NAF6A1 or call 1-800-643-4668



The new at&t

IPS

continued from page 38

don't make appointments. Also, we used a laughably small number of exploits — just three in all — and offered them at rates never exceeding 16% of each system's maximum packet-per-second capacity. That we saw security issues at all came as a surprise.

The three exploits are all well known: SQL Slammer, the Witty worm and a Cisco malformed SNMP vulnerability. We chose these three because they're all widely publicized, they've been around awhile, and they're based on User Datagram Protocol (UDP), allowing us detailed control over attack rates using the Spirent ThreatEx vulnerability assessment tool.

The IPS sensors we tested sit in line between other network devices, bridging and monitoring traffic between two or more Gigabit Ethernet ports. Given their inline placement, the ability to monitor traffic at high rates — even as fast as line rate — is critical. Accordingly, we designed our tests to determine throughput, latency and HTTP response time. We used TCP and UDP test traffic, and found significant differences in the ways IPSs handle the two protocols (see How we did it at www.nwdocfinder.com/5122).

Vendors submitted IPSs with varying port densities. FortiGate-3600 has a single pair of Gigabit Ethernet interfaces, while IPS 5500 has two pairs. The IPSs from Ambiron TrustWave, Demarc, NFR and TippingPoint offer four port-

See IPS, page 44

NetResults

Product	ipAngel-2500	Sentarus Network Security Sensor	FortiGate-3600	Sentivist Smart Sensor ES1000	TippingPoint 5000E	IPS 5500-1000
Vendor	Ambiron TrustWave www.atwcorp.com	Demarc Threat Protection Solutions www.demarc.com	Fortinet www.fortinet.com	NFR Security www.nfr.com	TippingPoint www.tippingpoint.com	Top Layer Networks www.toplayer.com
Price	$100,000.	Sensor $37,000; Sentarus Threat Protection System management application starts at $25 per node.	$30,000.	Sentivist Smart Sensor ES1000, $75,000; Sentivist Management Platform, $10,000.	TippingPoint 5000E, $170,000; Security Management System, $10,000.	$80,000.
Pros	Blocked all exploits in final tests; innovative, vulnerability-based configuration system.	Blocked all exploits in final tests; vendor contributes signatures to open source Snort community; fastest to develop missing Cisco SNMP signature; well-designed dashboard gives instant status.	Blocked all exploits in final tests.	Blocked all exploits in final tests; very fine-grained control over traffic detection and response.	Fastest performer for good (non-exploit) traffic; choice of fail-open and fail-closed modes; outstanding management interface overall.	Strong performer with one or two port-pairs; good anti-denial-of-service protection features; rate-based management tools are top of the pack.
Cons	Modest performance from beta hardware and drivers; initially missed Cisco SNMP exploit; weak forensics and alerting capabilites.	Relatively modest performer; searching for signatures is difficult; comprehensive forensics and analysis tools; weak IPS configuration, forensics and reporting.	Lower port density than other products in this test; some software versions flooded exploit traffic (fixed in final version supplied by vendor); initially missed Cisco SNMP exploit; integration of IPS into UTM Firewall lacks features and manageability.	Relatively modest performance; initially missed Cisco SNMP exploit; complexity of interface not for the casual user.	Forwarded exploit traffic under heavy load; disables logging when overloaded.	Forwarded some exploit traffic (possibly because of vendor misconfiguration); initially missed Cisco SNMP exploit; weak forensics capabilities.

One port pair configurations

The Breakdown	Top Layer	Ambiron TrustWave	TippingPoint	Fortinet	Demarc	NFR
Baseline forwarding rate **10%**	5	1.25	5	2.5	5	3.75
Forwarding rate under attack **15%**	5	5	4.25	4	3.25	1
Baseline latency **15%**	3.25	3.75	3.5	4	3.5	5
Latency under attack **15%**	5	5	3.25	3.5	1.5	1
Protection from attack **25%**	3	4	3	4	4	4
Usability **20%**	3.5	2.8	4.1	2	2.7	3.9
Total score	**3.94**	**3.75**	**3.72**	**3.38**	**3.28**	**3.21**

Two port pair configurations

The Breakdown	Top Layer	TippingPoint	Ambiron TrustWare	NFR	Demarc
Baseline forwarding rate **10%**	5	5	1	1	2
Forwarding rate under attack **15%**	4	3.75	1	1	1
Baseline latency **15%**	2.75	5	2.75	4.25	3.5
Latency under attack **15%**	5	2	5	1	1.5
Protection from attack **25%**	3	3	4	4	4
Usability **20%**	3.5	4.1	2.8	3.9	2.7
Total score	**3.71**	**3.68**	**2.97**	**2.82**	**2.64**

Four port pair configurations

TippingPoint	Ambiron TrustWave	NFR	Demarc
2.5	1	1	1
2.75	1.5	1	1
5	4.5	4.75	2.5
3.25	4	1	2.5
3	4	4	4
4.1	2.8	3.9	2.7
3.47	3.16	2.89	2.54

Scoring Key: 5: Exceptional; **4:** Very good; **3:** Average; **2:** Below average; **1:** Subpar or not available

ServerIronGT E-Series Takes Application Switching to New Heights

By Doing Things that PC Appliances Cannot

ServerIronGT E-Series

High Availability & Reliability

- Resilient switching and routing foundation
- Global load balancing for multi-site scalability and survivability
- Link aggregation
- Rapid and stateful session failover
- RSTP, VRRP for switch and router redundancy
- Redundant power supplies

Security

- DoS protection up to 4 million SYN/sec
- Wire-speed ACLs
- Application rate limiting
- Secure device management
- sFlow traffic monitoring

Rich Features

- Intelligent content switching using URL, HTTP, XML, cookies, SSL ID and others
- IP NAT
- RIPv2, OSPF routing

Flexibility & Manageability

- In-line, one-ARM and Direct Server Return modes
- Web, SNMP, INM and Cisco-like CLI

Superior Performance

- Up to 140,000 L4 connections/sec
- Application throughput from 2 to 12 Gbps
- Wire-speed Layer 2/3 forwarding
- Scalable processor performance

Scalability & Expandability

- Port expansion to:
  - 48 Gigabit Ethernet
  - 48 10/100 Mbps Ethernet
  - 4 10-Gigabit Ethernet

Uptime, scalability, performance and security are the watchwords for your network. The ServerIron® application switch is designed for this environment. Its advanced switch-based architecture features a scalable content switching engine with hardware-based DoS protection delivering the industry's most powerful and secure application switching solution.

PC Appliances Cannot Match the Power and Flexibility of the ServerIron

	ServerIron	PC Appliances
Performance upgradeability	✓	✗
In-service port expandability	✓	✗
10-GE support, >10 Gbps throughput	✓	✗
High-density direct server fan-out	✓	✗
Hardware-based connection management and DoS protection	✓	✗
Wire-speed L2/L3 forwarding and ACLs	✓	✗

FOUNDRY® NETWORKS

The Power of Performance™

The ServerIron Family of Products Also Includes:

ServerIron 450 and 850

ServerIronXL

ServerIronSA Accelerators

Foundry Networks, Inc. is a leading provider of high-performance Enterprise and Service Provider switching, routing and Web traffic management solutions including Layer 2/3 LAN switches, Layer 3 Backbone switches, Layer 4-7 Web switches, wireless LAN and access points, access routers and Metro routers.

For more information please call: US/Canada 1 888 TURBOLAN, International +1 408.586.1700 or visit our website at www.foundrynet.com/sie

IPS

continued from page 42

pairs. To ensure apples-to-apples comparisons across all the products, we tested three times, using one, two and four pairs of ports where we could.

One port pair

Our tests of single port-pairs are the only ones where all vendors were able to participate.

In baseline TCP performance tests (benign traffic only, no attacks), the Demarc, TippingPoint and Top Layer devices moved traffic at 959Mbps, near the maximum possible rate of around 965Mbps (see The IPS Torture Test, Scenario 1, page 44). With 1,500 users simultaneously contending for bandwidth and TCP's built-in rate control ensuring fairness among users, this is about as close to line rate as it gets with TCP traffic.

It was a very different story when we offered exploit traffic, with most systems slowing down sharply. The lone exception is ipAngel, which moved traffic at rates under heavy attack that were equal to or better than its rates in the baseline test. All others slowed substantially under heavy attack — and worse, some forwarded exploit traffic.

The IPS 5500 leaked a small amount of Witty worm traffic at all three attack rates we used — 1%, 4% and 16% of its TCP packet-per-second rate. The vendor blamed a misconfiguration of its firewall policy (vendors configured device security for this project). With its default firewall policy enabled, Top Layer says its device would have blocked exploits targeting any port not covered by the vendor's Witty signature.

The TippingPoint 5000E leaked a small amount of malformed Cisco SNMP traffic when it was offered at 4% and 16% of the device's maximum forwarding rate, even after we applied a second and third signature update.

Further, with attacks at the 16% rate, the TippingPoint device disabled all alerts (it continued to block exploits but didn't log anything) for 10 minutes. TippingPoint calls this a load-mitigation feature and says customers overwhelmingly prefer this setting to having the device shut down if it becomes overloaded.

We understand that device behavior during overload is ultimately a policy decision. For enterprises where high availability trumps security, the ability to continue forwarding packets is essential — even if it means a temporary shutdown of IPS monitoring. More-paranoid sites might block all traffic in response to an overload. In this test, the TippingPoint and NFR devices (and possibly others) explicitly give users a choice of behaviors, a desirable feature in our view.

In terms of HTTP response time, NFR's Sentivist Smart Sensor delivered Web pages the fastest, at an average of about 144msec for an 11KB object. This is the average time it took for each of 1,500 users to request and retrieve a Web page with a single 11KB object, with no attack traffic present. The NFR sensor also flew through the 1% and 4% attack tests, with response times lower than those for all other vendors' baseline measurements.

The IPS torture test: scenario 1

Vendors submitted IPSs with varying port densities. To ensure apples-to-apples comparisons across all products, we tested three times, using one, two, and four pairs of ports where we could. If no results are listed for a vendor in a particular test scenario, that is because the vendor did not supply that configuration. Because TCP comprises 95% of the Internet's backbone traffic, we emphasized the effects of attacks on TCP traffic in our tests. However, we also conducted tests with pure User Datagram Protocol (UDP) traffic, because that protocol is used by VoIP, streaming media, instant messaging, and peer-to-peer applications. Footnotes in red indicate there was a security issue associated with that result. Footnotes in blue indicate there was a logging issue associated with that result.

Scenario No. 1: testing with one port pair across all vendors

Throughput (Mbps)	Perfect device	Ambiron TrustWave	Demarc	Fortinet	NFR	TippingPoint	Top Layer
TCP baseline	965	672	959	937	382	959	959
TCP plus 1% attack	965	929	924	928	358	959	959 [1]
TCP plus 4% attack	965	929	799	821	308	959 [2]	954 [3]
TCP plus 16% attack	965	868	216	453	158	317 [4]	911 [5]
UDP baseline, 64-byte frames	1,524	41	144	127	1,223	1,235	624
UDP baseline, 512-byte frames	1,925	301	1,925	1,005	1,925	1,925	1,925
UDP baseline, 1518-byte frames	1,974	628	1,960	1,974	1,974	1,974	1,974
Latency (millisec)	**Perfect device**	**Ambiron TrustWave**	**Demarc**	**Fortinet**	**NFR**	**TippingPoint**	**Top Layer**
TCP baseline	N/A	372.11	430.50	326.43	144.05	399.50	447.02
TCP plus 1% attack traffic	N/A	262.50	397.68	326.68	158.30	398.05	418.25 [1]
TCP plus 4% attack traffic	N/A	252.82	409.05	1,272.95	192.52	393.16 [2]	368.25 [3]
TCP plus 16% attack traffic	N/A	325.70	15,607.59	2,865.32	11,522.86	8,170.68 [4]	375.61 [5]
UDP baseline	N/A	0.14	1.50	0.43	0.08	0.07	1.46
UDP plus 1% attack traffic	N/A	0.12	259.12	17.36	7.59	1.40	5.34 [6]
UDP plus 4% attack traffic	N/A	0.12	404.65	4.31	6.85	11.53 [7]	8.43 [8]
UDP plus 16% attack traffic	N/A	0.15	648.71	12.96	6.45	13.54 [9]	5.55 [10]

Footnotes: [1] Forwarded 86 Witty exploits; [2] Forwarded 1 Cisco malformed SNMP exploit; [3] Forwarded 362 Witty exploits; [4] Forwarded 1 Cisco exploit, disabled logging for 10 minutes; [5] Forwarded 370 Witty exploits; [6] Forwarded 280 Witty exploits; [7] Disabled logging for 10 minutes; [8] Forwarded 322 Witty exploits, incorrectly labeled some exploits as SYN floods despite pure UDP load; [9] Disabled logging for 10 minutes; [10] Forwarded 159 Witty exploits, incorrectly labeled some exploits as SYN floods despite pure UDP load.

Something went horribly wrong for the Sentivist device in the 16% attack test, however, with response times registering nearly 80 times higher than in the baseline test. It could be simply an anomalous result; response time didn't increase anywhere nearly as much in the two and four port-pair tests on the Sentivist device. Further, the device's latency spiked only when hit with exploit traffic at more than 60Mbps, suggesting a serious and dedicated denial-of-service (DoS) attack was underway. After we concluded testing, NFR says it identified and corrected a CPU oversubscription issue, but we did not verify this.

Among other devices, ipAngel's response time degraded the least as we ratcheted up attack rates. This isn't too surprising, considering its sensor's powerful hardware the vendor supplied for testing. The ipAngel sensor had eight dual-core Opteron CPUs.

It's important to note that all results presented here are averages over the three-minute steady-state phase of our tests. These averages are valid, but they don't tell the whole story. As dramatic as the reduction in the average performance was in some tests, actual results over time show an even sharper drop in response to attacks. (See TCP forwarding rates under attack, page 38).

All IPSs slowed traffic to some extent under our heaviest attack, but the degradation differed in terms of degree and duration. ipAngel's rates degraded the least, although the rate at the end of the test for this product was 824Mbps, more than 100Mbps lower than the system's 929Mbps rate at the beginning of the test. Top Layer's IPS 5500 did the best job of bouncing back to its original rate after an attack, but even so it momentarily slowed down traffic by more than 550Mbps, to less than 400Mbps. Whether users would notice this slowdown depends on the application. Something involving sustained high-speed data transfer (for example, FTP) would experience a brief slowdown.

The TippingPoint 5000E's rates dipped to 10Mbps under attack, down from around 400Mbps, and it's even worse for the others, with rates going down all the way to zero. The Demarc and NFR numbers suggest an overload, while the Fortinet device appears to recover, then falter again.

The sharp fall in TCP rates also has an effect on HTTP page response time (see HTTP response times under attack, www.nwdocfinder/5130). Response time — the interval between a client requesting and receiving a Web page — is only a few hundred milliseconds in baseline tests. Under our heaviest attack, however, many IPSs introduced delays running well into the seconds. Ambiron TrustWave and Top Layer IPSs did the best job of maintaining low and consistent response time under attack.

These results show that IPS devices have the potential to cause significant delays in network performance, way out of proportion to the amount of malicious traffic in the network. In effect, an IPS could be the instrument that delivers a self-inflicted DoS attack, where a small amount of attack traffic can make a gigabit network painfully slow for Web traffic and completely unusable for file and print service.

After testing concluded, Demarc said new performance parameters in the Bivio sensor hardware it uses would have dramatically improved its numbers. Unfortunately, time constraints prevented us from verifying that.

We also measured UDP throughput. We consider the UDP data less important than the TCP data, because UDP typically is a much smaller percentage of traffic on the Internet side of production networks, but these tests still are a useful way to describe the absolute limits of device forwarding and delay. If you plan to put the IPS deep in your network, UDP traffic from sources such as backups or storage servers could form the bulk of your traffic.

Most devices moved midsize and large UDP packets at or

See IPS, page 46

TICK TOCK
TICK TOCK
:-(
:-(

Can anyone stop this exploit?

Of the three exploits chosen for this test (the Cisco malformed SNMP vulnerability and the SQL Slammer and Witty worms), the SNMP one gave our IPS vendors the most trouble.

The SNMP exploit is a simple one: Many versions of Cisco IOS 12.0 to 12.3 will reboot when a valid SNMP message, such as a Get or Set, is sent to a destination port expecting an unsolicited message, such as a Trap.

For example, a Get query normally goes to User Datagram Protocol (UDP) Destination Port 161. If an attacker instead sends a perfectly well-formed SNMP query to Port 162 (the Trap port), vulnerable versions of IOS will reboot. Because reboot time on some devices takes minutes, an attack even at a very low rate could keep a vulnerable router, switch or access point off the network.

Cisco announced and patched the vulnerability in May 2004. Considering the exploit's age and high profile, we expected all IPSs to detect and block it without incident. To make sure our Spirent ThreatEx vulnerability-assessment tool was firing a valid attack, we tracked down a vulnerable version of IOS, loaded it on a Cisco router and crashed it repeatedly.

Only the TippingPoint 5000E IPS spotted the exploit in initial testing. The other five IPSs tested missed it. In several cases, vendors asked us for a traffic capture so they could write a signature.

Even the 5000E missed one highly improbable variation of the exploit during initial testing. IOS listens for unsolicited messages on UDP Port 162 and on one random port in the range of 49152 to 59152. The TippingPoint device blocks solicited messages sent to either port.

If the randomly chosen port is in use, however, IOS instead listens on a port in the range of 59153 to 65535. Initially, the TippingPoint device did not spot exploits offered to a port in this second high-numbered range. Note that the probability of this vulnerability occurring is extremely low.

TippingPoint wrote a new signature to cover this remote possibility, but it had the effect of forwarding a small number of Cisco exploits when offered concurrently with benign TCP traffic — even when offered to Port 162 (an exploit that TippingPoint previously blocked). TippingPoint gave us a second updated signature, but the problem persisted. TippingPoint has since issued a fix for this issue.

As we started heating up the technical-support lines for all the other vendors, the patched signatures showed up fast and furious. Some vendors rapidly developed a comprehensive signature that blocked any form of the exploit. Other vendors, reacting to our test, rushed the job and wrote signatures that were so vague as to virtually guarantee false positives and negatives.

What was interesting to us was how poorly the signature-writing process worked. Demarc Threat Protection Solutions delivered a signature for its Snort-based system, and to its credit, also con-

See Cisco exploit, page 48

The IPS torture test: scenario 2

Testing with two port pairs

Throughput (Mbps)	Perfect device	Ambiron TrustWave	Demarc	NFR	TippingPoint	Top Layer
TCP baseline	1,930	1,013	1,446	382	1,825	1,911
TCP plus 1% attack	1,930	990	1,310	351	1,830 [11]	1837 [12]
TCP plus 4% attack	1,930	937	782	307	1,340 [13]	1429 [14]
TCP plus 16% attack	1,930	759	498	205	1,340 [15]	1254 [16]
UDP baseline, 64-byte frames	3,048	82	288	712	1,226	605
UDP baseline, 512-byte frames	3,850	602	2,009	2,009	3,850	3,850
UDP baseline, 1518-byte frames	3,948	1,172	1,977	1,977	3,948	3,948
Latency (milliseconds)	**Perfect device**	**Ambiron TrustWave**	**Demarc**	**NFR**	**TippingPoint**	**Top Layer**
TCP baseline	N/A	268.07	158.03	146.26	71.70	274.42
TCP plus 1% attack traffic	N/A	269.05	169.73	162.89	86.11 [11]	84.95 [12]
TCP plus 4% attack traffic	N/A	304.24	365.64	194.34	1,001.69 [13]	179.64 [14]
TCP plus 16% attack traffic	N/A	460.65	16,692.43	7,074.89	1,062.49 [15]	1,338.22 [16]
UDP baseline	N/A	0.09	0.31	0.09	0.08	2.33
UDP plus 1% attack traffic	N/A	0.13	202.30	0.12	4.16 [17]	12.35 [18]
UDP plus 4% attack traffic	N/A	0.18	391.80	0.10	8.95 [19]	12.18 [20]
UDP plus 16% attack traffic	N/A	5.32	566.80	0.64	6.63 [21]	7.15 [22]

Footnotes: [11] Forwarded 9 Cisco malformed SNMP exploits; [12] Forwarded 174 Witty exploits; [13] Forwarded 13 Cisco exploits, disabled logging for 10 minutes; [14] Forwarded 524 Witty exploits; [15] Forwarded 57 Cisco exploits, disabled logging for 10 minutes; [16] Forwarded 1158 SQL Slammer, 1140 Witty, and 1138 Cisco exploits; [17] Disabled logging for 10 minutes; [18] Forwarded 199 Witty exploits, incorrectly labled some exploits as SYN floods despite pure UDP load; [19] Disabled logging for 10 minutes; [20] Forwarded 139 Witty exploits, incorrectly labled some exploits as SYN floods despite pure UDP load; [21] Disabled logging for 10 minutes; [22] Forwarded 33 Witty exploits, incorrectly labled some exploits as SYN floods despite pure UDP load.

IPS

continued from page 44

near the theoretical line rate. The two exceptions were FortiGate-3600, which moved midsize packets at about 50% of line rate, and ipAngel, which moved UDP traffic (for all packet lengths) at far lower rates than it moved TCP traffic. Ambiron TrustWave says its sensor used betas of interface device drivers and later versions show higher throughput and lower latency with UDP; we did not verify this.

As in the TCP tests, latency in the UDP testing also spiked sharply when we subjected most IPSs to attack, with hundredfold (or more) increases in delay not uncommon. The only exception was ipAngel, which delayed packets by roughly the same amount in the attack tests as in the baseline test. This could be attributable to the ipAngel's UDP throughput, which is much lower than that of the other devices in this test.

We gave all vendors an opportunity to review and respond to test results before publication. TippingPoint found in internal testing that latency would have been far lower had we measured at 95%, not 100% of the throughput rate. Top Layer asked for a smaller reduction in load (perhaps to 99.9%), and attributed its increased UDP latency to clocking differences between our test tools and its IPS.

While lower loads probably would have produced lower delays, we respectfully disagree with both vendors' suggestions, on two grounds. First, as described in RFC 2544 — the industry standard for network device performance benchmarking — latency is measured at the throughput rate and not at X percent of the throughput rate, where X is some number that produces "good" latency.

Second, neither vendor's device bears a sticker warning customers that rates should never exceed X percent of line rate. If vendors want to claim high throughput, they also should measure latency at the throughput level.

Two port pairs

In baseline TCP performance tests, the IPS 5500 was the fastest device, with the TippingPoint 5000E not far behind (see The IPS Torture Test, Scenario 2, this page). The Ambiron TrustWave, Demarc and NFR devices all moved TCP traffic at rates much further below the theoretical maximum than in the single port-pair tests.

The Top Layer and TippingPoint devices also produced the highest rates in the attack tests, but results were problematic. The TippingPoint 5000E forwarded a small amount of Cisco exploit traffic in all three of our attack tests, and disabled logging in our 4% and 16% attack tests. The Top Layer device forwarded small amounts of Witty worm traffic in all three attack tests. The issues for both vendors were the same as in the single port-pair tests: TippingPoint had a problem with the Cisco signature, and Top Layer had a problem with its firewall configuration.

The Sentarus sensor and ipAngel were the fastest IPSs among devices that did not forward any exploit traffic. The Sentarus came out on top when we offered attacks at 1% of the TCP rate, moving traffic at close to the baseline speed. The ipAngel was quickest in the 4% and 16% attack tests, though rates were about 10% and 25% lower, respectively, than in the baseline test.

HTTP response times also shot up dramatically under attack, though in some cases the delays were lower with two port-pairs than with one. This could be attributed to device architecture, in which IPS sensors use dedicated CPUs and/or network processors for each port-pair.

In the UDP tests, the TippingPoint and Top Layer IPSs were again the fastest, moving midsize and large frames at line rate. The Demarc and NFR devices were about half that fast: Both posted identical numbers, possibly because both use the same Bivio sensor hardware.

UDP latency was higher under attack than in the baseline tests, especially for Sentarus in the 16% attack test. However,

See IPS, page 48

Cisco exploit

continued from page 46

tributed the signature to the open source signature repository at the Bleeding Edge Snort Web site. Demarc's first attempt covered only Port 162, but it quickly added signatures to cover exploits offered to high-number ports. Demarc did a great job, even though it took them a few tries to get it right.

When ipAngel initially missed the Cisco exploit, Ambiron TrustWave delivered a signature that blocked the specific variant of the Cisco SNMP exploit we used in testing, but the signature probably would lead to false positives in a production setting. The ipAngel signature checks for any SNMP traffic sent to UDP Destination Ports 162 or 49152 to 65535. That let the device pass our performance test, but the signature also would generate false positives on any legitimate SNMP Trap. The company has since refined its signature.

We also discovered the drawbacks in combining IPS technology into unified threat management (UTM) firewalls, a difficult design to get right. Fortinet's FortiGate-3600 initially forwarded all exploit traffic, not just the Cisco SNMP attack. This was because of a UDP learning issue in the FortiGate UTM box, in which it would broadcast all traffic for which it had not yet seen destination MAC addresses. In this regard, FortiGate worked like an Ethernet bridge, not a security appliance. Fortinet corrected that behavior with new firmware, but the IPS still forwarded all exploits when we attacked at 16% of the system's capacity. It also forwarded the Cisco exploit at any offered rate when we used a high-numbered destination port. It took another firmware release to shut out the exploits for good.

NFR Security developed an effective signature after we sent its engineers a capture of the exploit traffic we used when its Sentivist Smart Sensor missed the exploit.

Top Layer's IPS 5500 initially forwarded Cisco exploit traffic. After we supplied the traffic capture, Top Layer supplied a pattern-matching signature that we found easy to evade. First, it detected only an SNMP Get message and not other solicited message types, such as Getnext, that also would cause reboots. Second, it covered only queries exactly 28 bytes long, when in practice SNMP message length is variable. Third, the signature covered only exploits sent to Destination Port 162 and not high-numbered ports.

Top Layer supplied additional signatures to cover the first two issues. As for listening on high-number ports, the company disagreed that an IPS would need to block these. Company engineers stated that firewall policies and/or router access-control lists should be sufficient to block this traffic.

That's a disingenuous argument, in our opinion. If firewalls always were configured perfectly, and if hosts always were patched fully, the need for signature-based IPSs would disappear. Because we were testing IPSs on their ability to do their jobs, it didn't seem relevant that most enterprises would have intended to block SNMP, Witty, and SQL Slammer at their external firewall. More importantly, the Witty and SQL Slammer worms became notorious exactly because people didn't have firewalls in place and properly configured.

These results don't mean that IPSs aren't useful at increasing the security of enterprise networks. What they do mean is that an IPS can be only one component in a defense-in-depth security strategy, and it's much better to eliminate the vulnerabilities in your network by patching software and firmware than it is to depend on an IPS to provide protection.

— David Newman and Joel Snyder

The IPS torture test: scenario 3

Testing with four port pairs

Throughput (Mbps)	Perfect device	Ambiron TrustWave	Demarc	NFR	TippingPoint
TCP baseline	3,860	1,730	1,514	382	3,434
TCP plus 1% attack	3,860	1,692	1,268	351	3,402 [23]
TCP plus 4% attack	3,860	1,538	694	307	2,317 [24]
TCP plus 16% attack	3,860	1,317	350	205	1,875 [25]
UDP baseline, 64-byte frames	6,095	130	541	712	1,210
UDP baseline, 512-byte frames	7,699	1,203	2,556	2,009	4,018
UDP baseline, 1518-byte frames	7,896	2,400	2,899	1,977	4,454
Latency (milliseconds)	**Perfect device**	**Ambiron TrustWave**	**Demarc**	**NFR**	**TippingPoint**
TCP baseline	N/A	160.91	166.27	146.26	112.25
TCP plus 1% attack traffic	N/A	167.80	237.12	162.89	110.72 [23]
TCP plus 4% attack traffic	N/A	194.55	630.03	194.34	627.8 [24]
TCP plus 16% attack traffic	N/A	636.18	15,285.89	7,074.89	491.99 [25]
UDP baseline	N/A	1.24	343.63	0.11	0.04
UDP plus 1% attack traffic	N/A	7.13	205.78	0.10	28.02 [26]
UDP plus 4% attack traffic	N/A	8.64	388.81	0.11	9.93 [27]
UDP plus 16% attack traffic	N/A	16.61	566.74	0.11	5.85 [28]

Footnotes: [23] Forwarded 1280 Cisco malformed SNMP exploits; [24] Forwarded 1128 Cisco exploits; [25] Forwarded 795 Cisco exploits, disabled logging for 10 minutes; [26] Disabled logging for 10 minutes; [27] Disabled logging for 10 minutes; [28] Disabled logging for 10 minutes.

IPS

continued from page 46

excluding that one result, latency generally rose less with two port-pairs under attack than with one — again, possibly caused by distributed processing designs.

Four port pairs

With four pairs of Gigabit Ethernet interfaces (thus, rates theoretically capable of rising as high as 8Gbps), this was the acid test for IPS performance.

The TippingPoint 5000E was hands-down the fastest IPS in our TCP baseline tests (see The IPS Torture Test, Scenario 3 this page). It moved a mix of applications at 3.434Gbps, not far from the test bed's theoretical top rate of 3.8Gbps, and about twice as fast as the next quickest sensor, ipAngel.

In our attack tests, the TippingPoint 5000E again leaked small amounts of Cisco exploit traffic and also disabled logging in the 16% attack test.

Of devices with no security issues, ipAngel was fastest. As in tests with two port-pairs, ipAngel's TCP forwarding rates degraded as we ratcheted up attack rates, but on the other hand it did not leak any exploit traffic.

Most of the devices increased HTTP response time under attack, especially in the 16% attack test. In the worst case, response time through Sentarus spiked from 166msec in the baseline test to more than 15 seconds in the 16% attack test. That may have been attributable to a tuning parameter in the Bivio sensor, according to Demarc. Unfortunately we only learned of this parameter after testing concluded.

TippingPoint's IPS was also the fastest in our UDP tests. In baseline tests it moved large packets at 4.454Gbps, the fastest single rate in our tests. It was also the top performer in baseline tests of short and medium-length packets.

Latency skyrocketed for multiple devices once we combined benign and attack UDP traffic. For example, the TippingPoint 5000E delayed benign UDP traffic by nearly 30 seconds in a test with attacks at 1% of its capacity, and the device also disabled logging in all three of our attack tests. The other products also slowed traffic by huge margins over the baseline test. The IPS with the best UDP latency under attack was Sentivist, not just with four port-pairs but indeed in all tests.

If the test results say anything, it's that performance and security are two very different goals, and — at least with these devices — the goals often may not bear any sensible relationship to one another.

These tests turned up two different kinds of IPSs: devices that move traffic at very high rates, and devices that block attacks but aren't the speediest performers. Picking the right IPS comes down to finding the right balance between security and performance.

Newman is president of Network Test, an independent engineering services firm in Westlake Village, Calif. He can be reached at dnewman@networktest.com.

Network World *gratefully acknowledges the vendors that supported this project. Spirent Communications supplied its Spirent ThreatEx, Avalanche, Reflector, SmartBits and AX/4000 test tools, and engineer Chuck McAuley assisted with ThreatEx configuration. Apcon supplied an Intellapatch virtual patch panel that tied together the test bed. And Red Hat supplied its Red Hat Enterprise Linux operating system, used on test bed management servers.*

Much more IPS online

The full lowdown on IPS usability. www.nwdocfinder.com/5124.

Can an IPS product really cover you? www.nwdocfinder.com/5150.

Find out how we tested these products. www.nwdocfinder.com/5122.

VIDEO: Walk through our test bed. www.nwdocfinder.com/5151.

IPS Buyer's Guide. www.nwdocfinder.com/4051.

NETWORKWORLD

SUBSCRIPTIONS

The new network switch
Next-generation switches will combine security, application awareness and policy enforcement PAGE 32.
NETWORKWORLD
February 6, 2006 ■ Volume 23, Number 5
The leader in network knowledge ■ www.networkworld.com
Juniper/NetScreen deal bears fruit
SSG 520 has security, routing features that could give Cisco gear a good run.
Cisco looks to grab broader security role
NETWORKWORLD CLEAR CHOICE
2006
Help is on the way
FREE SUBSCRIPTION

Each week ***Network World*** delivers an extensive line-up of product, service and industry news, analysis, case studies, buyer's guides, expert opinion and management advice that Network IT Executives rely on to get their job done.

Your FREE subscription will include...

- New product information and reviews that break through vendor hype and put you in control of your technology purchases
- Implementation strategies and security tips and tricks that you can use to improve your infrastructure and boost your company's competitive standing
- Tried-and-true management strategies to help you boost your network career
- An insider's view on how your competitors are using new technology to their business advantage

Plus our Special Signature Series Issues—Each Signature Series issue provides insights, opinions and information on an important aspect of the industry to give you the clearest picture of the current trends and trendsetters in the Network IT market.

To subscribe visit:
apply.nww.com/free05

Network World, Inc., | 118 Turnpike Road, Southborough, MA 01772 | (508)460-3333

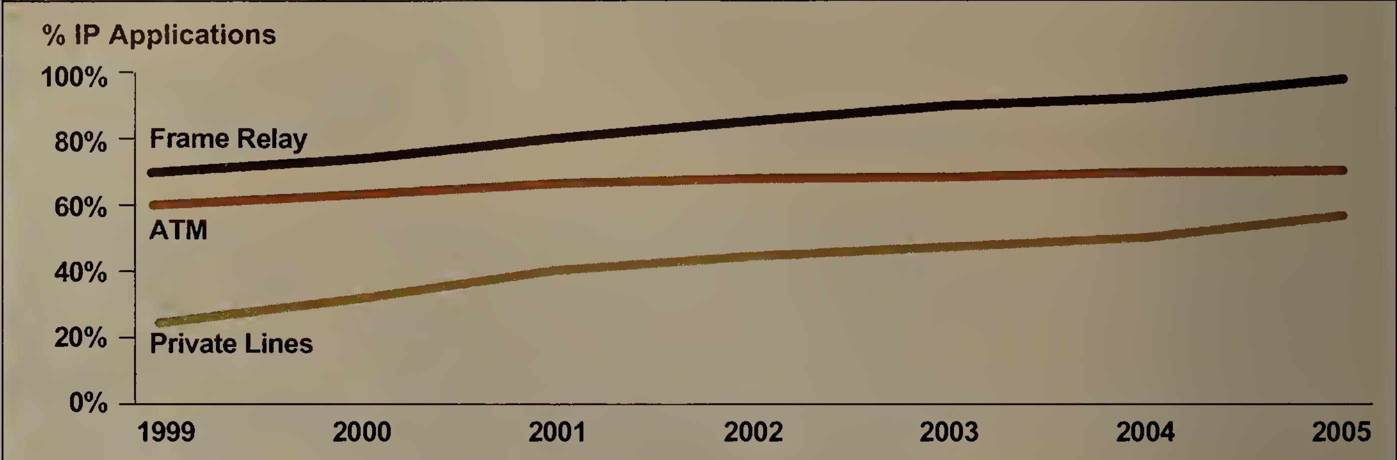
A New Era Dawns in Global Carrier Services

From VoIP and VPNs to wide-area Ethernet, MPLS is spawning an array of new services for large enterprises and SMBs alike.

It's A CHICKEN OR EGG SCENARIO: Is MPLS driving demand for new services, or are the services the reason that nearly every major carrier has chosen MPLS as the new base of their network infrastructure?

IP Convergence Trends

IP applications now account for the majority of traffic on frame relay, ATM and private lines provisioned for enterprise customers in the U.S. Non-IP data protocols (such as SNA and IPX), plus legacy voice and video applications account for the balance of traffic transported via these services.



SOURCE: VERTICAL SYSTEMS GROUP, WESTWOOD, MASS.

Whatever the case, it seems clear that legacy technologies such as frame relay and private lines are well on their way out the door. In fact, a Nemertes Research benchmark done this spring found that frame relay deployments within respondent companies have dropped from 78% in 2004 to 46% today.

MPLS is not a new technology. "At this point, most providers are using some form of MPLS with their backbone," says Jeff Young, a senior analyst at Burton Group, a network research company in Midvale, Utah. But with MPLS-based services finally gaining ground since the original trickle of services began in the early 2000s, the promise of MPLS seems to be finally coming to fruition. "This is still in some manner of deployment, but the proliferation of standards sitting on top of MPLS is working at making good on that promise," says Young.

And as services multiply, enterprise interest seems finally to be reaching critical mass: Nemertes found that 42% of its benchmark respondents reported using MPLS, compared with 24% in 2004. Moreover, nearly 10% more were planning on implementing MPLS-based services within the year.

In response, carriers are expanding their array of services, using MPLS as a base architecture. "They have a choice of either offering services and being competitive, or losing the customer," says Steve Taylor, editor/publisher of Webtorials, a telecom education and research site. "It's also where the margins are."

> "No longer is VoIP being offered only by specialist providers and VoIP pioneers, but by all types of providers in all regions of the world."
>
> **Stéphane Téral,** principal analyst, Infonetics Research

MPLS-based services are attractive for a number of reasons. Carriers are generally pricing them lower than existing data services, as they try to migrate users away from legacy technologies. MPLS also offers quality-of-service (QoS) support, giving companies better control of their service levels. It also helps reduce capacity planning, as switched MPLS traffic means that it's easier to achieve a meshed network configuration without having to discretely link between every possible combination of sites. "Companies can just buy connections to the MPLS network from sites A thru Z, and they don't have to worry about what's in middle," says Young.

Given this ongoing shift, how can companies best rethink their carrier service mix? Clearly, decisions must be flavored by questions of cost and ease of use, but carriers are delivering new services targeted at a wide array of companies, whether sprawling enterprises or small to midsize businesses. The following are some of the more intriguing technologies and services that are drawing corporate interest across the board.

VoIP

"Voice over IP is one of the significant drivers for new fully meshed IP services," says Erin Dunne, director of research at Vertical Systems Group, a network research company in Westwood, Mass. "If you want to do VoIP, you have to make a service change [from frame relay or private lines]. It's IP-based and you're most likely looking at MPLS." Given its popularity, carriers are responding with increased capacity and services. According to a report by the market research firm Dell'Oro Group in Redwood Shores, Calif., the sales of VoIP equipment to carriers will increase from 2004's $1.6 billion to $4.7 billion by 2010.

"No longer is VoIP being offered only by specialist providers and VoIP pioneers, but by all types of

NTT Communications - The Quiet Giant

One of the largest global carriers may be a company you've never heard of—NTT Communications. If you haven't run across NTT Com yet, here are four reasons to find out more.

1. Network Reach. Simply put, NTT Com's Global IP Network has tremendous global breadth and reach. NTT Com is the largest carrier of IP traffic between the U.S. and Asia. The network currently boasts the industry's largest dedicated Internet bandwidth of 95G bit/sec between Japan and the U.S., 22G to Europe and 33G to Asia Pacific, providing end users with fast, smooth global Internet connections.

This high-quality Tier 1 IP backbone has been enhanced both in terms of bandwidth, to support end users' broadband Internet usage, and in terms of direct connection to major ISPs in Asia, the U.S., Europe and Oceania.

2. Innovative Products. NTT Com has a history of introducing ground-breaking products and services. This summer, the company launched 10G bit/sec Ethernet (10GigE) to the NTT Com Global IP Network, which covers three continents.

"In keeping with its global technology leadership, NTT Communications has raised the bar again by offering 10GigE to customers spanning three continents. The global reach of this ultra-high-speed Ethernet service across the U.S., Europe and Asia is a first in the industry," said Joshua Holbrook, senior analyst at Yankee Group, a Boston consultancy.

NTT Communications

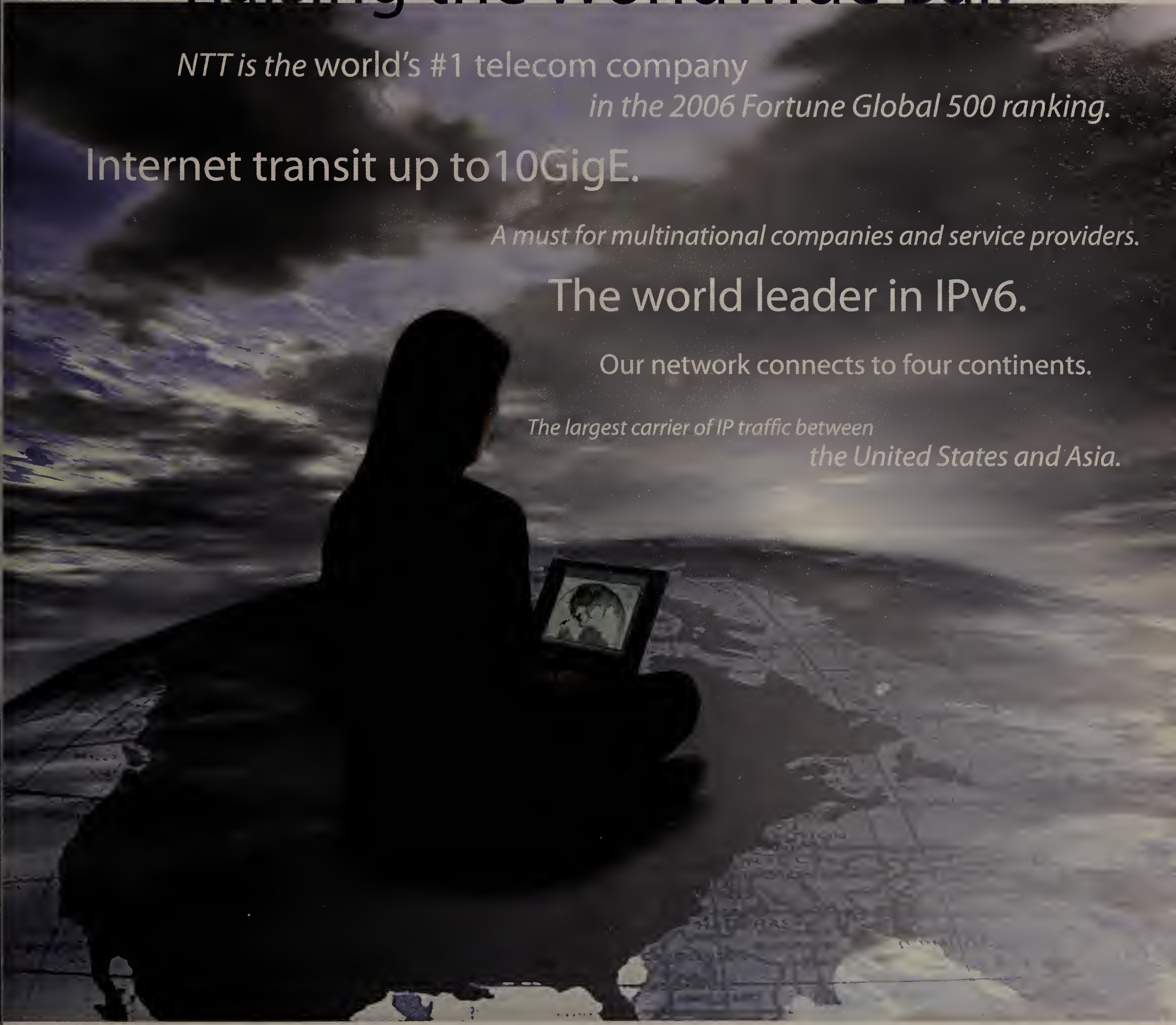
The service offers customers guaranteed reliability and accountability through financially backed service level agreements. And it works with both IPv4 and IPv6. Indeed, NTT Com is a leader in IPv6 technology, and it operates the world's largest Tier 1 IPv6 backbone, spanning Asia, Europe, North America and Australia.

3. Financial Stability. NTT Com is a wholly owned subsidiary of NTT, which is ranked as the world's largest telecom company by revenue in *Fortune* magazine's 2006 Global 500 survey.

4. Global Consistency. NTT Com's ability to offer a single autonomous system number (ASN 2914) globally is key for large multinational customers or companies that do international routing. It allows ubiquitous route views and consistent routes to customers that require services across multiple regions, and provides for consistent global operations and best practices. The single ASN also means global customers can deploy technologies such as MPLS Traffic Engineering (MPLS-TE), which doesn't span ASN borders effectively.

Learn more about the NTT Communications Global IP Network. **Visit http://us.ntt.net/innovator or call (877) 8NTT-NET.**

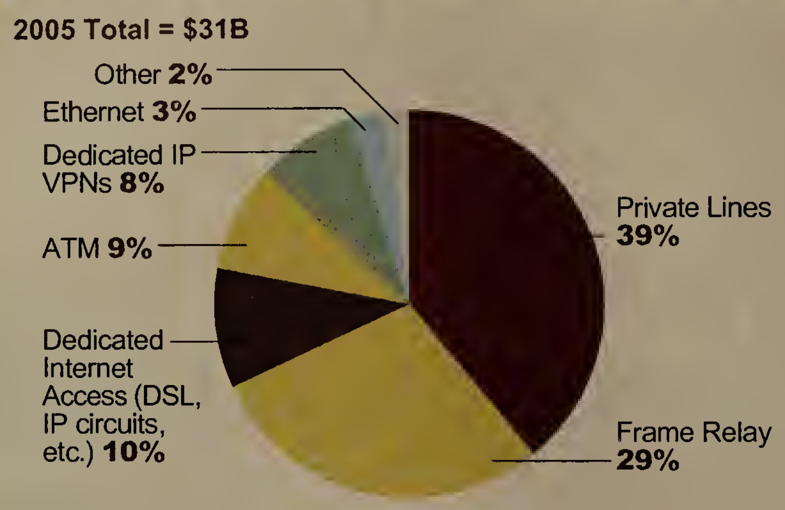
Raising the Worldwide Bar.


NTT is the world's #1 telecom company
in the 2006 Fortune Global 500 ranking.
Internet transit up to10GigE.
A must for multinational companies and service providers.
The world leader in IPv6.
Our network connects to four continents.
The largest carrier of IP traffic between
the United States and Asia.

Know more at **877-8-NTT-NET** or visit us at **http://us.ntt.net/innovator**

***NTT** Communications* | **NTT America**

The Data Service Revenue Picture



SOURCE: VERTICAL SYSTEMS GROUP, WESTWOOD, MASS.

Legacy data services accounted for more than three-quarters of all U.S. business data service revenue last year, but emerging dedicated IP VPN and Ethernet services have the most substantial revenue growth for 2006, according to industry watchers at Vertical Systems Group. They say the dedicated IP VPN market alone represents a cumulative $35 billion opportunity for U.S. service providers between 2004 and 2009.

providers in all regions of the world," says Stéphane Téral, principal analyst for service provider VoIP, IMS (IP Multimedia Subsystem) and FMC (Fixed Mobile Convergence) at Infonetics Research in Campbell, Calif. "Next-gen voice services have elevated from lab curiosity to market reality." Research from Infonetics' report, "Service Provider Plans for Next Gen Voice & IMS," shows that service providers expect both incoming and outgoing VoIP traffic to nearly double over the next year, with international long-distance traffic growing the fastest.

This could bode well for companies that have a growing international presence, as many of the overseas carriers are expanding VoIP services aggressively. Teral says that while carriers in high teledensity areas such as North America and Western Europe are adding VoIP as an alternative to existing services, carriers in areas with less teledensity are deploying next-generation voice technologies as their primary platform.

While VoIP doesn't have to use an MPLS-based IP infrastructure—it will also run over the open Internet—there are drawbacks to the latter approach. The chief attraction of running VoIP over MPLS is the ability to apply QoS standards through MPLS' packet marking. "MPLS does have factors for distinguishing levels of service, while the open Internet doesn't, and very likely won't in the future," says Young.

VPN

Virtual private network (VPN) services are the other major driver to MPLS implementation, says Dunne. "VoIP and VPN are prime MPLS-based services targeted at frame relay customers," she says. "They represent a very nice upgrade."

Like VoIP, VPN can be run over the open Internet as well as a carrier's MPLS-based network, and there are benefits to both choices.

"Internet-based VPNs have cost and ubiquity going for them—you can get anywhere the service has Internet access," says Dunne. "The downside is depending on the Internet for connectivity. You can't control the cloud."

She says that these services often work well for cost-conscious companies with a hodgepodge of Internet access services that don't rely on the VPN for mission-critical applications.

The other choice is to sign up for a more private-style VPN using a managed MPLS network. "The price is higher, but you get differentiated quality of service through MPLS," says Dunne. "You're paying for increased reliability."

Both options, she adds, have done quite well over the past couple of years.

Ethernet-Based Services

Along with MPLS, the other big service trend involves the growth of Ethernet-based services. "We're seeing a move not only to MPLS but to Ethernet-based services, primarily for the simplicity," says Taylor. NTT America, for example, announced this summer the availability of 10G bit/sec Ethernet (10GigE) to the NTT Communications Global IP Network. The offering marks the first time that such a high-speed bandwidth connection has been made available to a wider service area.

"Ethernet is where the hype is and also where the interest is—and this is one place where I suspect the market revenue will follow the hype," Dunne says. "You would previously cringe when thinking of using Ethernet for anything going out-

> **"VoIP and VPN are prime MPLS-based services targeted at frame relay customers. They represent a very nice upgrade."**
> **Erin Dunne,** director of research, Vertical Systems Group

OPNET Modeling Tools Take the Risk Out of Network Design

When it comes to rolling out new products and services, carriers find themselves in a classic risk/reward dilemma. "The service providers we talk to are caught among three pressure areas," says Ed Sykes, senior vice president and chief scientist at OPNET, a network and application management software maker in Bethesda, Md. "They have to accelerate the delivery of a new service to capture market share, but at the same time, they have to do it right—and they have to be as cost-effective as possible."

Carriers are finding that a duo of innovative products from OPNET can help them effectively manage those risks.

SP Guru Network Planner. SP Guru Network Planner builds high-fidelity behavioral models of Layer 2/3 networks, including routers, switches, protocols and traffic. "By making changes in the software model, you can predict what would happen when you make changes in the real network," Sykes says. The tool allows service providers to accurately examine various what-if scenarios, allowing them to make better risk/reward choices. If a provider wanted to roll out voice over IP (VoIP), for example, it could use SP Guru Network Planner to simulate the impact on the network of various uptake rates, allowing for more accurate capacity planning.

OPNET®
Making Networks and Applications Perform™

SP Guru Network Planner is essential for service providers implementing MPLS-based virtual private networks (VPN), migrating from circuit-switched to packet networks, planning for service "survivability" or deploying 3G wireless services. The intelligence embedded in SP Guru Network Planner represents the most advanced technology available for planning and engineering service provider networks.

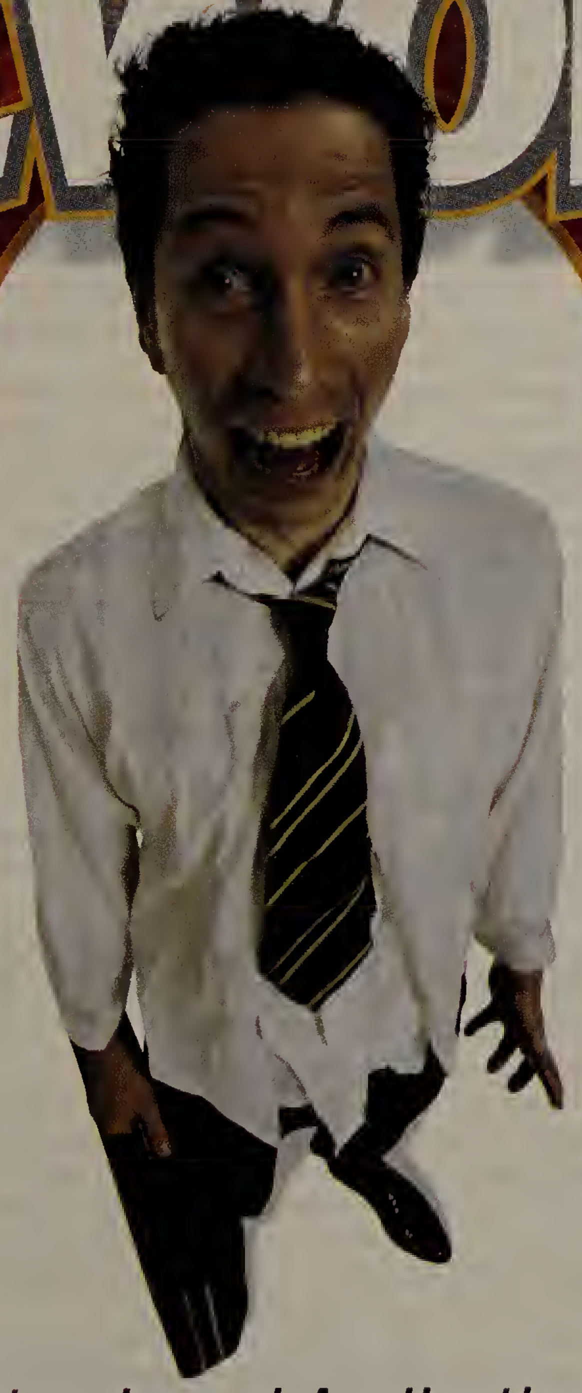
SP Guru Transport Planner. Looking to the future, many service providers are betting on intelligent optical network technologies to pave their entry into new markets and reduce their operating costs. Network equipment manufacturers, in turn, are seeking ways to demonstrate the benefits of their optical products.

SP Guru Transport Planner, like SP Guru Network Planner, is a modeling tool that enables service providers and network equipment manufacturers to design resilient, cost-effective optical and SONET/SDH networks. Its multi-layered network presentation, broad technology support, and cutting-edge optimization and design capabilities make SP Guru Transport Planner an invaluable resource for network architects and planners.

Moreover, while OPNET's two products work well alone, they are even more powerful as a team. "Each stands alone, but they complement each other," says Sykes. "Integrated, they provide additional value."

For more information, visit **OPNET at www.opnet.com**

"It's not the network!"



Prove it with OPNET ACE

OPNET ACE is the most powerful solution for rapid performance troubleshooting. It shows you exactly how network, system, and application behavior affect end-to-end performance. With ACE, you can pinpoint the source of a problem, so time and money aren't spent in the wrong places.

The most successful organizations in the world rely on OPNET's advanced analytics for networks, servers, and applications.

Making Networks and Applications Perform™

Best of the Tests NetworkWorld '05 Winner

Network Computing Company to Watch 2004

OPNET®

Forbes 2004 Best Small Companies

Winner Best of Show Networld Interop 2002

CONTACT OPNET TODAY

info@opnet.com • www.opnet.com • +1-240-497-3000

Cisco Systems® | Technology Developer Partner

NASDAQ: OPNT

side the business because of overhead, but there's so much bandwidth now and the cost is so low, it's really not an issue any more."

Companies love the idea of extending the reach of such a well-known networking protocol that runs on commodity equipment. "The learning curve is zero," says Dunne. "With an Ethernet switched service, you just plug the LAN into a little box and it just goes."

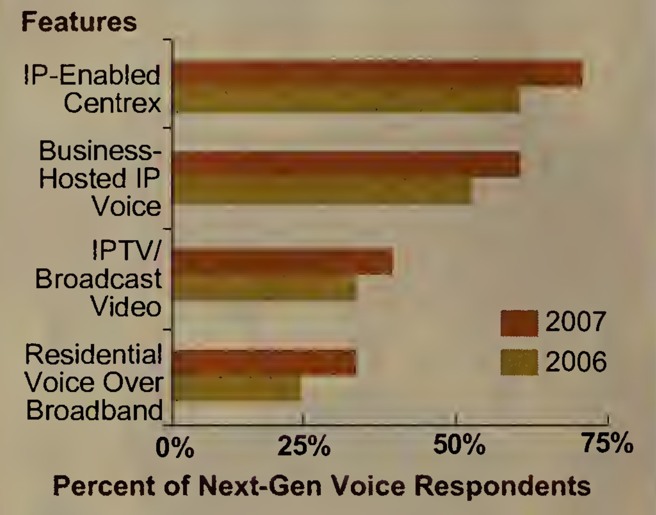
New Ethernet services have been booming. Metro Ethernet, which offers high-bandwidth Ethernet over MPLS in localized areas, is one such product, as typified by AT&T's Ethernet Switched Service - Metropolitan Area Network. "Metro Ethernet has been around for several years, but I'm starting to see it become more mainstream and see a growing range of services offered," says Webtorial's Taylor.

The reach of Metro Ethernet is expanding. AT&T's metro area footprint, for example, extends across the continental U.S., with many buildings "On-Net" in approximately 100 metropolitan cities. But its reach is ultimately confined by the reach of fiber, which it requires to run. In response, carriers are introducing Ethernet services that run at slower speeds on the more ubiquitous copper wiring. "The hot part of the market right now is the sub-10M bit/sec and copper-based Ethernet services," Dunne says. She estimates that only 11.7% of U.S. companies have fiber connections, leaving a large market that would be interested in the other Ethernet services.

BellSouth Corp. is one of the first large providers to roll out midrange Ethernet services, offering 2M, 4M and 8M bit/sec, as well as higher speeds.

Taylor says that the midrange Ethernet options should be particularly appealing to small businesses and companies that want to maintain Ethernet connections between corporate headquarters and branch offices. "Hopefully, it'll make life simpler and easier," he says.

Wholesale VoIP Service Features Offered by Service Providers



SOURCE: INFONETICS RESEARCH, CAMPBELL, CALIF.

There are some remaining issues to be ironed out, such as the interoperability of Ethernet with legacy services, interoperability of different carrier networks, and making Ethernet widely available over copper wire. But "Ethernet should nicely follow the hype if the service providers can work out the issues," Dunne says.

At the other end of the spectrum is Virtual Private LAN Service (VPLS), which uses MPLS to enable Ethernet-based wide-area VPNs. With VPLS, all users and devices appear to be connected to the same Ethernet LAN, even if they are physically in different locations. "VPLS is like the Holy Grail," says Dunne. "A lot of service providers are already offering it, but it's hard to do." Integration issues and the necessity of building new infrastructure has carriers rolling out VPLS more deliberately as compared to many other new services.

Managed Services

In addition to offering transport, analysts are also seeing carriers branching out to offer value-added services that address areas including security and performance.

Taylor cites managed firewall and security services as good options for carrier-based services. "Corporations spend a lot of energy on firewalls, and the fundamental question that gets answered way too seldom is whether this is something that is handled most appropriately inside the corporate network. Is it something the network service provider can do?" Taylor says he's also seeing services rolled out in the area of application acceleration: "The whole idea is to reevaluate the extent to which you should be your own Bell, so to speak."

One option that Burton Group's Young likes for companies that run their network as a cost center is to go with a virtual network operator such as Vanco PLC or Virtela Communications, Inc. "These companies buy wholesale from the big providers and provide exchange points themselves," says Young. "They'll completely operate the network for you."

He also likes this option for companies that need to establish an international presence but lack the expertise to do so. "It's become my favorite option if you don't have a lot of international experience," Young says.

While there are plenty of ancillary services available, Taylor is surprised at the slow uptake by customers. Managed services sometimes get associated with outsourcing, and IT executives approach the concept with caution. That concern should wane as confidence in these still-new services grows.

In the final analysis, the proliferation of new IP-based carrier services could finally signal the long-touted convergence of voice and data. But it'll still take time, says Young. "These changes are like big ships and big ships don't turn very fast," he says. "But slowly and surely, people are beginning to plan what they want to do about the new connectivity."

And the carrier services will be ready when they are.

A Breakthrough Approach for MPLS-VPN

Businesses today demand an ever-expanding list of requirements of their networks: facilitating real-time applications like VoIP or video; connecting remote locations; improving productivity; enhancing sales; supporting resource sharing; managing complex security issues. But the bottom line is the same: Enterprise customers expect high network performance and robust applications at a lower cost...without sacrificing functionality and reliability.

MPLS-VPN has become the standard for today's corporate networks. A fully meshed Layer 3, any-to-any connectivity, MPLS-VPN emphasizes routing and forwarding and provides CoS to ensure QoS and prioritization across applications. Where Layer 2 solutions depend on customer premise equipment, MPLS-VPN puts this demand on the carrier class infrastructure.

According to Sam Mansour, Senior Data Network Architect for Inter-Tel NetSolutions®, customers have become aware of MPLS' CoS and "application-aware" capabilities that enable prioritization of applications over other best-effort offerings.

"When you have traffic congestion you need stability for the WAN fabric so data delivery is streamlined. With other environments, latency is more of an issue," Mansour explains. "Also, most of the enterprise customers we deal with are looking for disaster recovery and network survivability. This is becoming a crucial feature.

"In addition, MPLS-VPN does two key things for any enterprise network. First, it addresses applications to avoid congestion, and second, it streamlines the IP traffic," says Mansour. "In the end, you get stability and efficiency."

Providers are keenly aware of positioning their network services for total cost of ownership with customers and prospects. Yet, in a communications world where equipment comes from one source, financing from another and network management by a different company, customers aren't always left with the optimal service situation.

Inter-Tel uniquely provides a single point-of-accountability for demanding enterprise customers through its Axxess® 5000 and soon-to-be released 7000 families of converged communications platforms and its Managed Services program. Inter-Tel also offers feature-rich applications to maximize productivity and improve business processes by enabling industry leading presence, messaging and collaboration tools.

In addition, with its Tier 1, carrier-neutral Network Services offerings, Inter-Tel NetSolutions offers a bundled approach to enabling IP-centric communications. By combining an MPLS network solution with its INOC Web portal, Inter-Tel NetSolutions provides network monitoring and management to ensure maximum reliability.

Contact Inter-Tel today to learn more about Flat Rate MPLS-VPN and for a FREE comprehensive evaluation of your communications network. 1-800-894-7026.

INTER-TEL®

Our Customers Tell It Like It Is.

NPL Construction

Inter-Tel® Customer for Over 7 Years.

"**Right now we have 23 offices in 11 states.** Our connectivity between offices five years ago was just a modem connection.

We got together with Inter-Tel and put a Wide Area Network in place so that all of our offices could interconnect on a five digit calling number. Our converged NetSolutions® WAN allows us to combine our voice and data over the same infrastructure while maintaining high service levels and user satisfaction. This is especially beneficial because many of our offices are in remote locations; other solutions would simply be impractical from both a cost and functionality perspective.

The people at Inter-Tel are amazing. We call the NetSolutions® number and they pretty much take care of everything – which is very valuable to me since I only have six people on my IT staff. That makes a world of difference."

Mike McConnell
Director of Information Services, NPL Construction Company

SuperShuttle®

SuperShuttle®

Inter-Tel® Customer for Over 10 Years.

"**We're in 18 major airports.** Our communication with each one of those locations is vital to properly handling our customers.

(Inter-Tel) provided me something that I couldn't do in any other system. They became part of our infrastructure. Their NetSolutions® services, along with their phone, gave me the single point of accountability I was looking for to help us manage our business.

I have very little downtime with any of these systems which is extremely important to our operations since we're 24 hours a day/365 days a year. I can't afford downtime.

It's easy for me to compliment Inter-Tel: One, for their reliability both in their products and their network. And, also, for their customer service – their employees are very, very customer service oriented. Their team being able to say "yes" to me whenever I have a crisis is extremely important. I find that refreshing."

Linda Paquin
V.P. of Reservations & Telecommunications, SuperShuttle Transportation Systems

▶ To learn more about Inter-Tel's value-driven communications systems and solutions, visit www.inter-tel.com

INTER-TEL
NetSolutions
1-800-[illegible]
www.inter-tel.com

InfoWorld

VIRTUALIZATION EXECUTIVE FORUM

VirtExecForum.com

September 25-26, 2006
Roosevelt Hotel
New York City

ENABLING VIRTUALIZATION ACROSS THE ENTERPRISE

InfoWorld's Virtualization Executive Forum provides a clear roadmap for building out a virtual-oriented architecture. Early adopters are already experiencing the benefits of virtualization across the enterprise. Learn from the challenges they've faced and the benefits they've achieved.

ATTEND THIS TWO-DAY CONFERENCE WITH A FOCUS ON:

- Leveraging virtualization for business and IT agility
- Best practices for testing in virtual labs
- Virtualization and enterprise applications
- Charting the migration from physical to virtual
- Technical and organizational challenges of implementing virtualization

Save $200 when you register by September 20th and receive discount pricing

Use discount code NWWP

LEARN TO PUT THEORY INTO PRACTICE FROM THE IT PROFESSIONALS WHO SPEAK FROM FIRST-HAND EXPERIENCE

TONY BISHOP
Senior Vice President & Director of Product Management, **Wachovia**

DR. JEFFREY JAFFE
Chief Technology Officer, **Novell**

ANDI MANN
Senior Analyst, **Enterprise Management Associates**

STEVE YATKO
Managing Director of Global R&D IT Group, **Credit Suisse First Boston**

VirtExecForum.com

CORNERSTONE SPONSOR
Novell.

PLATINUM SPONSORS
EMC² where information lives®
intel
PolyServe™
redhat.
vmware®

GOLD SPONSOR
Data Synapse
EMULEX
IBM.
Microsoft®

E-MAIL NEWSLETTER SHOWCASE:

Storage in the enterprise

Disaster recovery, five years later

BY MIKE KARP

A reporter asked me recently what the major impact of Sept. 11 was on the storage industry. And her follow-up question was even better: "If backup, recovery, and disaster planning became so important, how come so many storage companies are not doing well?"

Even though we had all that optical fiber running to the New Jersey side of the river where all the disaster-recovery sites were located, that wasn't enough.

Most obvious was that a lot of data had been kept on desktop and laptop machines, and that almost none of the data had been protected. Many companies were able to failover to their disaster-recovery sites with ease, and were immediately able to access the data on their servers. But the data on the desktops was lost.

Vendors able to offer protection to desktop and laptop machines increased their value in the marketplace. They addressed a need, and if their products were any good, they had a better shot at success than their competitors.

Vendors or service providers that can assist in disaster planning and in the recovery of critical corporate information seem to be doing quite well these days. And so are companies that can provide some demonstrable improvement in the way we do backups and recoveries. Companies with a viable continuous data protection offering, whether it is a new product or an enhancement, seem to be doing better than competitors that lack that capability. Continuous data protection is capturing mindshare, and with it, market share.

Crafting solutions that match up to real problems seems to work pretty well. But why then are some companies not doing well in a market that is enabling others to achieve record numbers? Because, the reality is that although the tides may rise and the tides may fall, only seaworthy craft will remain afloat.

You can't count on market trends to make your company successful. You can be prepared against the various eventualities. If you're a boat owner, you can have your craft checked out by the Coast Guard. If you are a corporate executive, stop drinking the corporate Kool-Aid and get out there among the users to find out what they really want. Remember that no matter how good the members of the marketing department may be, by the time information eventually makes its way to your office what you hear you may not really be what they said.

Think of the "telegraph" game where the first child whispers into the ear of the second child, the second child whispers what she heard into the ear of the third, and when the message reaches the last person it may be distorted.

Don't screw up the corporate messaging because you didn't hear what the market really said.

Karp is senior analyst with Enterprise Management Associates.

He can be reached at mkarp@enterprise management.com.

E-MAIL NEWSLETTER SHOWCASE: IT Careers and Training

How one IBMer got out of a career rut

BY LINDA LEUNG

Darryl Solie spent 24 years at IBM developing the company's server and storage products. He had little contact with customers. He'd gained broad technical knowledge in his role but he felt stagnant in his career. That was until five years ago when IBM set up its Technology Collaboration Solutions group where he became one of a few IBM engineers to go onto customer sites and talk to them about ways in which the vendor could work with the customer to extend the customer's own technology.

Although the change in job role was scary at first, Solie says the move "rejuvenated my enthusiasm for technology," and he believes the model of working with customers on "collaborative innovation" will open many doors for those seeking careers in the engineering, technology and business fields.

Based in Rochester, Minn., Solie as IBM distinguished engineer describes himself as a chief systems architect, helping customers such as Mayo Clinic and Boeing to combine their technologies with IBM's for specific applications.

The move was not without its challenges as the learning curve was pretty steep, he says. He remembers diving head first without formal negotiation training into intensive week-long meetings with IBM business folks and execs from the customer company to thrash out a $100 million deal.

"We negotiated on the delivery expectation, the terms and conditions of the delivery and the legal aspects of it. All of the different aspects [of the deal] were promised on the fundamentals of IBM technology. The meetings got so intense because the negotiations were so challenging. Negotiations went from 8 a.m. to 10 p.m. and later, for a week. During the whole week we [IBM folks] had to take time out six or eight times to discuss what our position was," he says.

Despite the lack of formal training, Solie says the experience opened his eyes to contract negotiations where preparation, the ability to listen carefully to the customer, and knowing what is negotiable, are part the art of negotiations.

Solie says there was no formal training when the group was first established because the area of technology collaboration was so new. But now IBM has in place a formal mentoring program in which Solie and other engineers mentor IBM veterans who have been at the company 15 to 20 years, and newbies who have been with the company for less than five years. There is some formal classroom training, Solie says, but mostly it is one-to-one or one-to-two training centered around discussing aspects of deals that they may be working on and client visits. Solie is usually still the sole technical engineering representative in meetings with prospective customers.

nww.com

In your in-box

Sign up for this or any of *Network World's* many other e-mail newsletters.

www.nwdocfinder.com/1002

Solie says his role is best suited to technologists who are comfortable dealing with new people. "There are engineers who really want to do just that — engineering. But there are others who have a different sort of soft/interpersonal skills."

For people starting out in their IT careers who are interested in customer-facing roles, Solie suggests taking communications and public speaking classes. For IT pros who have been around for a while but want to rejuvenate their careers as Solie did but may feel uncomfortable with new people, do as Solie did — join a golf club to help yourself feel comfortable in non-technical social environments.

"Anytime there's a chance for a new horizon most people will find it exciting and rewarding," he says. ■

RECLAIM YOUR NETWORK

Order a free evaluation unit at www.barracudanetworks.com/nww

Spam, Spyware, IM and Virus protection at an affordable price.

- No per user license fees
- Powerful, enterprise-class solution
- Handles up to 20 million messages per day

BARRACUDA NETWORKS

SPAM, SPYWARE AND IM FIREWALLS

2005 WELL-CONNECTED AWARDS WINNER

CRN star search 2005

SC MAGAZINE 2005

Business 5 Star PARTNER PROGRAM WINNER 2006

Network Computing Editor's Choice

[illegible] Networks [illegible] Spyware Firewall are [illegible] trademarks or registered trademarks of Barracuda Networks, Inc. and/or its subsidiaries [illegible]

POWERFUL EASY TO USE AFFORDABLE

Aggressive reseller program available. Get more info by visiting
www.barracudanetworks.com/nww or 888-ANTI-SPAM

E-MAIL NEWSLETTER SHOWCASE: Branch office best practices

Branch office challenges hit the spotlight

BY ROBIN GAREISS

The number of calls, e-mails, and general inquiries I've been receiving about the branch office has done the hockey-stick incline in the past few months. At the same time, you've probably noticed a lot of vendors discussing their products, services, and plans for the branch office.

Yes, IT executives and managers — not to mention business-unit leaders — are paying more attention to the branch office. What's driving this increased interest? Two key factors:

First, data center consolidation projects are well underway or nearly finished at many organizations. Now that the databases and applications reside in a central location, the IT and network staffs must make sure the infrastructure to and in the branch is up to par.

They need to ensure that the remote employees can access data and applications in a consistent, predictable, and efficient manner.

In fact, Nemertes found that user expectation for branch-office performance vs. headquarter and large regional office performance will become nearly even by 2007.

What this means is that employees in small branch and even home offices will expect nearly the same performance as they receive when they're in headquarters. Their patience for slow access lines, inconsistent application response time, and outages is drastically waning, so calls to the help desk and complaints to IT will be on the rise.

Second, business-unit leaders are recognizing their remote workers must be as productive as possible — and that a solid IT infrastructure enables this productivity. Companies are adding branch offices at an average growth rate of 8.9% annually, and they continue to hire people to work at branch locations.

To stay competitive, they need collaborative tools and a solid IT infrastructure.

During the next few weeks, I will discuss some of the products and services that will help organizations meet these branch office challenges. Many of the e-mails and calls I receive are from those asking for help in selecting the right products, designing the right architecture, and determining who should be the decision-maker. Let me know at robin@nemertes.com what's on your mind, and I'll do my best to incorporate the answers in the next series of columns.

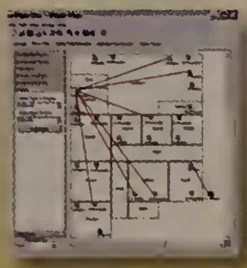
Gareiss is executive vice president and senior founding partner for Nemertes Research. She can be reached at robin@nemertes.com

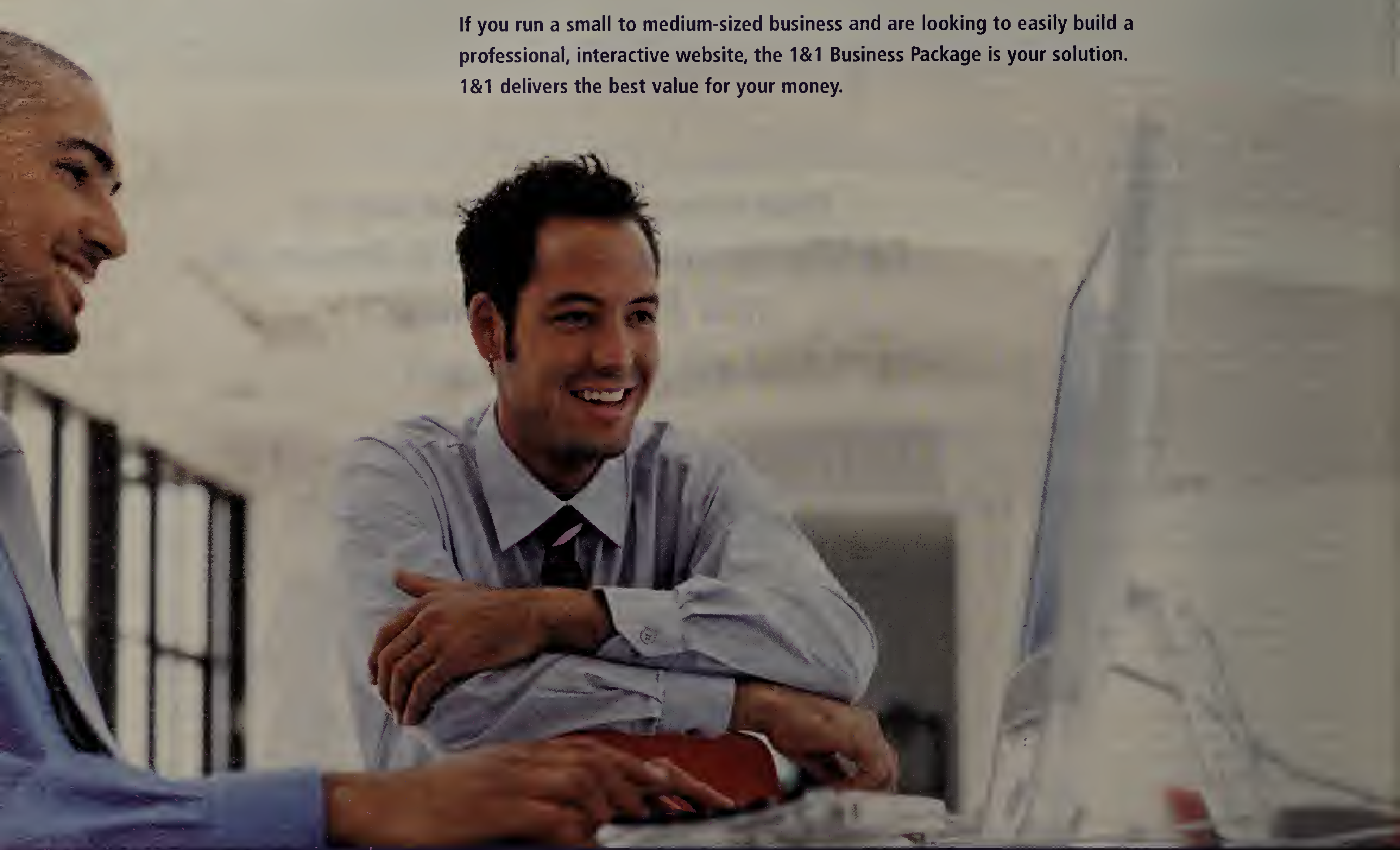
nww.com

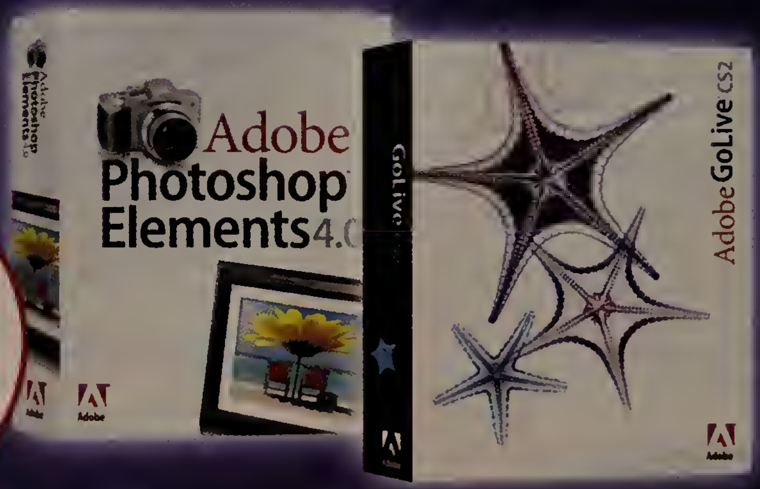
In your in-box

Sign up for this or any of *Network World's* many other e-mail newsletters.

www.nwdocfinder.com/1002






Adobe Photoshop Elements 4.0
Adobe GoLive CS2

the Best...

Save 25%

On All 1&1 Shared Hosting Packages

Offer ends September 30, 2006

Compare for yourself!

	1&1	YAHOO!	Go Daddy
	BUSINESS	STANDARD	PREMIUM
Included Domains	3	1	$1.99/year with purchase
Web Space	100 GB	10 GB	100 GB
Monthly Transfer Volume	1,000 GB	400 GB	1,000 GB
E-mail Accounts	2,000 IMAP or POP3	500 POP3	2,000 POP3
Mailbox Size	2 GB	2 GB	10 MB
RSS Feed Creator	✓	–	$4.99/month
Blog	✓	✓	$2.99/mo. for ad-free blogs
Search Engine Submission	✓	✓	$29.99/year for submission and optimization
Search Engine Optimization	90-Day Trial	90-Day Trial	
Map & Driving Directions	✓	✓	–
Website Builder	18 Pages	✓	Freeware
Flash Site Builder	18 Pages	–	–
Photo Gallery	✓	✓	✓
Dynamic Web Content	✓	✓	–
Web Statistics	✓	✓	✓
E-mail Newsletter Tool	✓	$10/month	$9.99/year
In2site Live Dialogue	✓	–	–
Chat Channels	✓	–	✓
Form Builder	✓	✓	–
Premium Software Suite	✓	–	–
90-Day Money Back Guarantee	✓	–	–
Support	24/7 Toll-free Phone, E-mail	24/7 Toll-free Phone, E-mail	24/7 Phone, E-mail
Price Per Month	$9.99	$19.95	$14.99
SPECIAL OFFER	25% off for 1 year!	25% off for 2 months	–
TOTAL/YEAR	$89.91	$229.42	$179.88

We offer a variety of hosting packages to fit your needs and budget.

Discount offer ends September 30, 2006 and applies to 1&1 Internet, Inc.'s shared hosting packages. Visit 1and1.com for details. Prices based on a comparison of regular Linux prices, effective 7/25/2006. If you choose to receive the Premium Software Suite you must commit to a one-year contract for the package you choose. $6.99 shipping & processing fee applies. Product and program specifications, availability, and pricing subject to change without notice. Go Daddy is a registered trademark of Go Daddy Software,Inc.; Yahoo! is a registered trademark of Yahoo! Inc.

1&1

or visit us now **1and1.com**

The virtues of volunteering

CISO reaps rewards from his work with a user organization.

BY ELLEN MESSMER

Taking on volunteer work for an organization pledged to IT security can pay off handsomely in solidifying business partnerships, fostering corporate security and earning kudos from your boss. But volunteering in key positions will inevitably take time away from your job — meaning you face working longer hours to compensate.

Working extra hours to compensate for time spent volunteering is a fact of life for Paul Simmonds, CISO at ICI, a England-based manufacturer of paints and specialty chemicals that has 355 business sites worldwide connected via a global WAN.

His day job involves deciding how security will be implemented on behalf of tens of thousands of ICI employees. In his volunteer capacity,Simmonds is a member of the board of the Jericho Forum, a user-based organization of mostly large, global firms, such as BP, Procter & Gamble and Qantas.The forum's mission is to collaborate on finding ways to facilitate e-commerce without traditional security measures — such as perimeter firewalls and proxies — being needed for security. For about a year, vendors have been permitted to join, but they don't have privileges to vote on the forum's documents and IT architecture papers.

Simmonds' volunteer work of advocating for the Jericho Forum's philosophy — known as deperimeterization — and publicly speaking about it at trade shows and other meetings has consumed about 5% of his time, he says.

To Simmonds, it's more than worth it because he believes the forum's collaborative efforts are critical to the future of doing business on the Internet, where financially motivated cyberattacks are growing and consumers appear increasingly afraid of online commerce.

"Use of the Internet is based on trust, and we're using it for communications and business," he says. "I can't do that on the mass level I need to [if I use] today's technology."

Traditional VPNs, firewalls and proxies are seen by the Jericho Forum as barriers to e-commerce rather than facilitators, and the organization's membership is eager to identify alternative security methods.

The forum's membership — which has grown from 30 to 100 companies since Simmonds started his public-speaking engagements two years ago — holds face-to-face meetings once a month and two conferences a year, in North America and Europe.

The impact of this volunteer work is such that he typically works longer hours. "It's often a 60-hour week," he says. His volunteer work is backed by ICI's management, however, which subsidizes his expenses associated with the forum because the company views it as a means of finding better ways to do business online. "Management feels strongly about Jericho Forum," Simmonds notes.

Applying knowledge

Although it remains voluntary, Simmonds' work with the forum is having an effect on the strategic direction of ICI's own networks, because the ideas he brings back to his corporate management are becoming accepted as a template for future technology procurements.

Simmonds points out that the Jericho Forum's members have been effective at sharing their views and writing papers aimed at making it clear to the vendor community what they like and don't like about today's products. Those views are summed up in white papers on subjects such as basic architecture, VoIP, wireless and content filtering.

Not only has the Jericho Forum membership articulated its views in position papers, but some members, including ICI, are taking steps to wean themselves from perimeter, VPN-based firewalls or other technologies.

"BP Amoco just moved 18,000 users off the intranet and onto the Internet with no firewall at all, authenticating at the application level," Simmonds says. "Boeing is doing the same thing."

In "Internet Filtering and Reporting," a position paper published in July, the forum advocates moving content and URL filtering further from the corporate intranet to the Internet. That's an idea being embraced in practice at ICI.

"We're using that idea as a basis for an RFP that we sent to 15 vendors in May, including AT&T, BT, MessageLabs, ScanSafe, Verizon and others," Simmonds says. "We're saying, move URL and content filtering, and analysis of spoofed Web sites, and do that filtering in the cloud."

ICI hopes to conclude a contract for outsourced content filtering in time to have the service in place for its operations by early next year.

Future agenda

Upcoming Jericho Forum projects include a critical assessment of network-access control technologies available. The forum's strategy papers often take many months to complete, but the organization's growing clout means its opinions are becoming heard more widely by companies and vendors.

That's good news to Simmonds, who has worked with diplomatic urgency to sway vendors to give deperimeterization a fair hearing. "Cisco came in about six weeks ago to Jericho Forum, and IBM is actively involved, too," he says. That kind of participation should foster a dynamic between enterprise customer and vendor to build IT products that are simpler and more effective in securing networks that depend on the Internet for e-commerce. ■

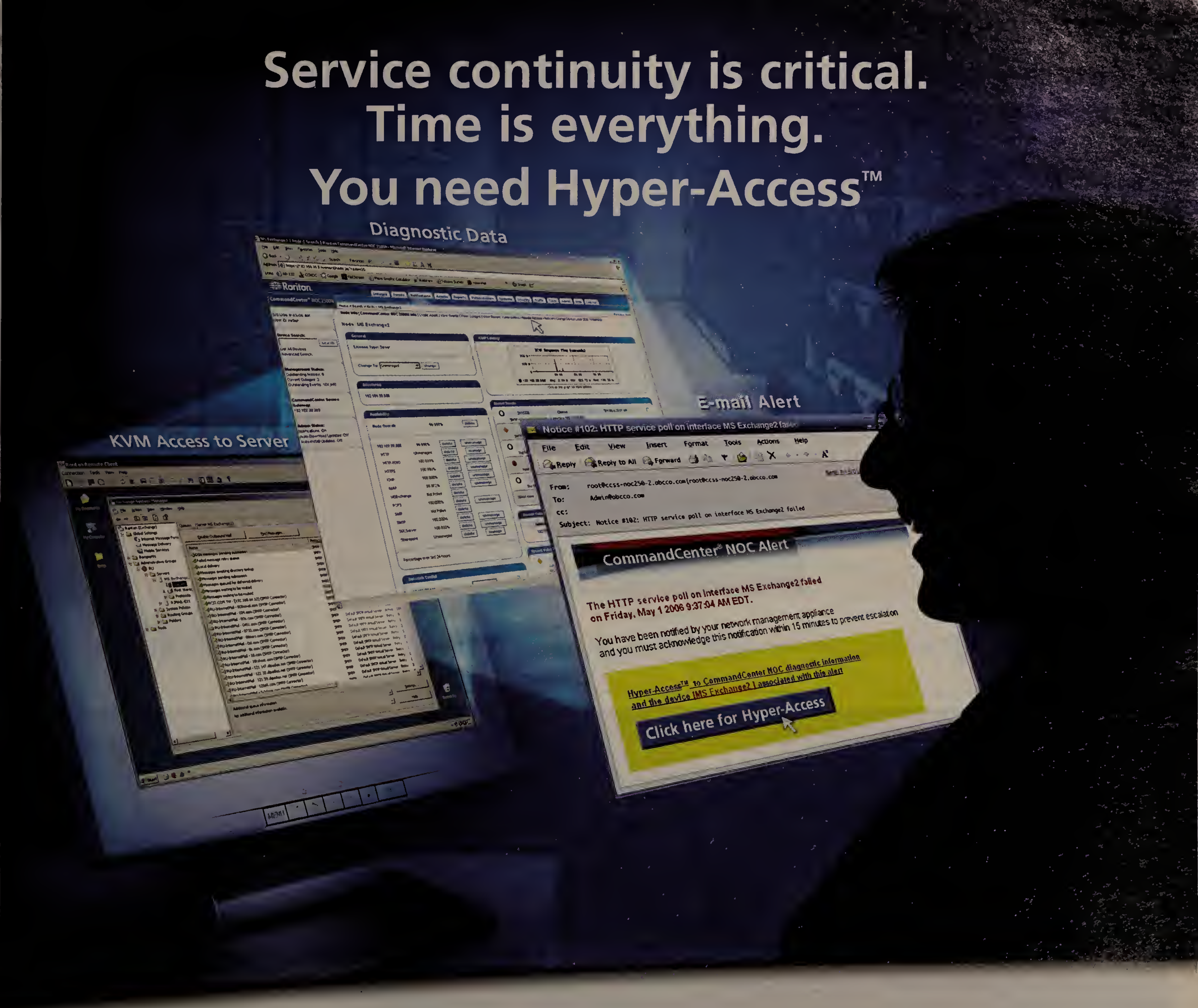
Jericho Forum at a glance

Mission:	To develop a security architecture and design approach that will let businesses grow safely and securely in an open, Internet-driven networked world.
Host:	The Open Group
Working groups:	Requirements, Solutions, Stakeholders.
Membership:	Includes more than 50 international blue-chip user organizations, such as BP, Rolls-Royce, Royal Mail and Qantas.
Position paper topics:	Internet filtering and reporting, wireless, voice over IP, protocols, architecture, commandments.

"Use of the Internet is based on trust, and we're using it for communications and business."

Paul Simmonds, CISO, ICI

MICHAEL WILLIAMS


Service continuity is critical.
Time is everything.
You need Hyper-Access™
Diagnostic Data
KVM Access to Server
E-mail Alert
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
Click here for Hyper-Access

Notice #102: HTTP service poll on interface MS Exchange2 fa

From: root@ccss-noc250-2.abcco.com[root@ccss-noc250-2.abcco.com
To: Admin@abcco.com
cc:
Subject: Notice #102: HTTP service poll on interface MS Exchange2 failed

CommandCenter® NOC Alert

The HTTP service poll on interface MS Exchange2 failed on Friday, May 1 2006 9:37:04 AM EDT.

You have been notified by your network management appliance and you must acknowledge this notification within 15 minutes to prevent escalation

Hyper-Access™ to CommandCenter NOC diagnostic information and the device [MS Exchange2] associated with this alert

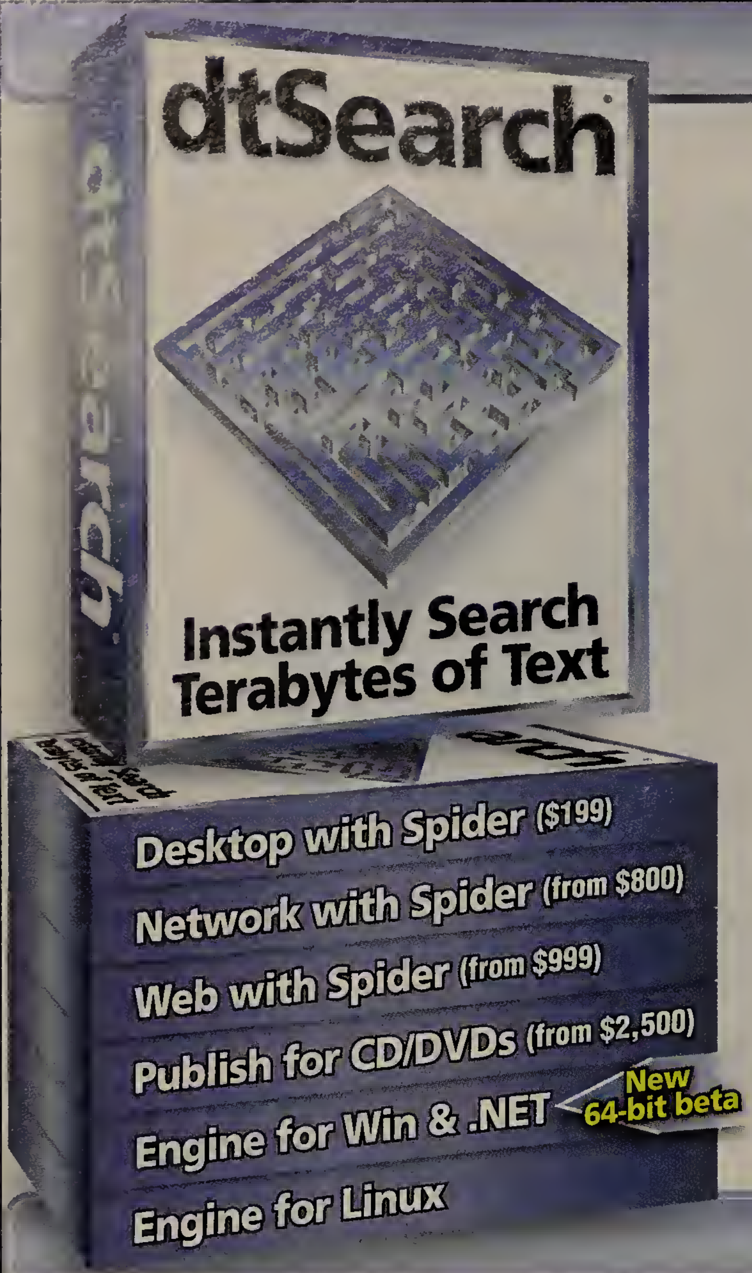
CommandCenter® management products - everything you need to diagnose and repair faults at your fingertips.

Hyper-Access. Only from Raritan. It's the revolutionary way our CommandCenter management products combine proactive management with secure, remote access to get you right to the heart of problems. When trouble occurs anywhere in your network, CommandCenter NOC sends you an e-mail alert with a Hyper-Access link to both diagnostic information about the device that triggered the alarm PLUS instant, click-and-fix, in-band and out-of-band access to the distressed device – all without leaving your chair. It's all part of the future of IT infrastructure management. From Raritan.

www.HyperAccessControl.com

Raritan.
When you're ready to take control.®

The e-mail notification in the picture shows graphics for emphasis. The notifications in the current CC-NOC release are plain text, compatible with any SMTP email client.



- Desktop with Spider ($199)
- Network with Spider (from $800)
- Web with Spider (from $999)
- Publish for CD/DVDs (from $2,500)
- Engine for Win & .NET New 64-bit beta
- Engine for Linux

Instantly Search Terabytes of Text

- over two dozen indexed, unindexed, fielded data and full-text search options
- highlights hits in HTML, XML and PDF, while displaying links, formatting and images
- converts other file types (word processor, database, spreadsheet, email and attachments, ZIP, Unicode, etc.) to HTML for display with highlighted hits
- Spider supports static and dynamic Web content, with WYSWYG hit-highlighting
- API supports .NET/.NET 2.0, C++, Java, SQL databases. New .NET/.NET 2.0 Spider API

dtSearch® Reviews

- "Bottom line: dtSearch manages a terabyte of text in a single index and returns results in less than a second" – *InfoWorld*
- "For combing through large amounts of data, dtSearch "leads the market" – *Network Computing*
- "Blindingly fast"– *Computer Forensics: Incident Response Essentials*
- "Covers all data sources ... powerful Web-based engines"– *eWEEK*
- "Searches at blazing speeds"– *Computer Reseller News Test Center*
- "The most powerful document search tool on the market"– *Wired Magazine*

For hundreds more reviews — and developer case studies — see www.dtsearch.com

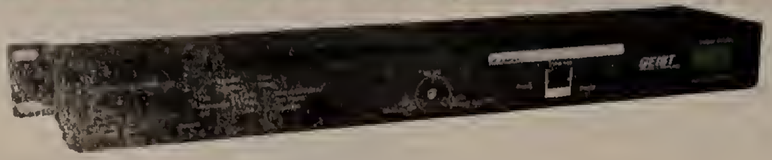
Contact dtSearch for fully-functional evaluations

The Smart Choice for Text Retrieval® since 1991

1-800-IT-FINDS • www.dtsearch.com

There are better ways to cool your data center.

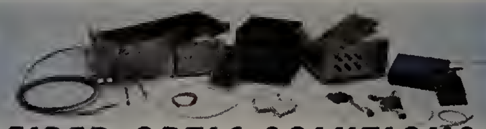
The New Geist Variable Speed Fan Controller blows away the competition.



Maintain optimal cabinet temperature while reducing fan noise and conserving energy. The Geist Fan Controller takes real-time temperature measurements and automatically adjusts the fan speed accordingly to protect your equipment.

Learn more at AFCOM Booth #328

www.racsense.com



FIBER OPTIC SOLUTIONS

- T1/E1 & T3/E3 Modems
- RS-232/422/485 Modems ond Multiplexers
- IBM 3270 Coox, AS400 Twinox, ond RS6000 Modems ond Multiplexers
- LAN - Arcnet/Ethernet/Token Ring
- Video/Audio/Hubs/Repeaters
- ISO-9001
- USB Modem ond Hub

S.I.TECH
Toll Free 866-SITech-1
630-761-3640, Fax 630-761-3644
www.sitech-bitdriver.com or www.sitechfiber.com

D-Series - Cost Effective Server Racks

Designed to provide housing for servers, hubs, routers and network equipment, along with structured cabling components, these enclosures provide a highly attractive profile in a robustly constructed cabinet. **770-496-4000**

www.optimaeps.com

Optima EPS
Cabinets & Enclosures
An ELMA Company

ONE PHONE SYSTEM
for many branch offices

mck communications
A Citel Company

MCK EXTenders
New, Refurb,
Installation, Support

RICKENBACKER
communications

ph: 978.475.7200 *fx:* 978.428.6200
www.rickenbackercommunications.com

Reading someone else's issue of *Network World?*

Subscribe today and receive your own 1-year subscription for FREE –

a $129.00 value!

Go to http://apply.nww.com/free for your free subscription.

NETWORKWORLD

Editorial Index

Advertiser Index

These indexes are provided as a reader service. Although every effort has been made to make them as complete as possible, the publisher does not assume liability for errors or omissions.

*Indicates Regional Demographic

Network World, Inc.

118 Turnpike Road, Southborough, MA 01772
Phone: (508) 460-3333

TO SEND E-MAIL TO NWW STAFF
firstname_lastname@nww.com

Evilee Ebb, CEO/Publisher
John Gallant, President/Editorial Director
W. Michael Draper, Chief Operating Officer
Eleni Brisbois, Administrative Planning Manager

FINANCE
Mary Fanning, Vice President Finance
Paul Mercer, Finance Manager
Betty Amaro-White, Event Finance Manager

HUMAN RESDURCES
Eric Cormier, Human Resources Manager

CUSTOM MEDIA
Michael Siggins, Associate Publisher/Custom Media

MARKETING
TerryAnn Fitzgerald, Sr. Director of Customer Experience
Jeanne Seltzer, Marketing Communications Manager
Barbara Sullivan, Senior Research Analyst
Judy Schultz, Marketing Design Manager
Cindy Panzera, Marketing Designer
Deborah Vozikis, Design Manager Online

PRODUCTION SERVICES
Greg Morgan, Senior Director, Production Services
Karen Wallace, Senior Director, Advertising Operations
Mike Guerin, Manager of Production Technologies
Jami Thompson, Sr. Production Coordinator
Veronica Trotto, Online Operations Coordinator
Jane Wilbur, Online Ad Traffic Coordinator
Maro Eremyan, Advertising Coordinator
Christina Pankievich, Advertising Coordinator

CIRCULATIDN
Richard Priante, Senior Director of Circulation
Judy Cloutier, Membership Services Specialist

RESEARCH
Ann MacKay, Research Director

DISTRIBUTION
Bob Wescott, Distribution Manager/(508) 879-0700

IDG LIST RENTAL SERVICES
Amy Bonner, Account Executive
P.O. Box 9151, Framingham, MA 01701-9151
Toll free: (800) 434-5478 ext. 6026/Direct: (508) 370-0826
Fax: (508) 370-0020

SEMINARS, EVENTS AND IDG EXECUTIVE FDRUMS
Neal Silverman, Executive V. P., Events & Executive Forums
Mike Garity, Sr. Director, Marketing & Bus. Development
Dale Fisher, Director of Operations
Jacqueline DiPerna, Senior Event Coordinator
Caroline Keough, Event Planner
Karen Bornstein, Account Executive
Andrea D'Amato, Sr. National Sales Director
Jennifer Sand, Regional Account Manager
Cedric Fellows, Regional Account Manager
Grace Moy, Exhibit Sales Manager
Debra Becker, Dir., Marketing & Audience Development
Sara Nieburg, Senior Marketing Manager
Cassandra Valentine, Registration & Customer Service Mgr.
Buster Paris, Marketing Specialist

DNLINE SERVICES
Kevin Normandeau, Exec. Vice President/General Mgr., Online
Dan Gallagher, Sr. Director, Audience Development
Mary McIntire, Sr. Manager, Audience Development
Adam Gaffin, Executive Editor, Online
Jason Meserve, Multimedia Editor
Sheryl Hodge, Associate Online News Editor
Jennifer Moberg, Online Marketing Program Manager
Chrystie Terry, Manager of Online Audience Development

CLIENT SERVICES
Sharon Stearns, Director of Client Services
Frank Coelho, Client Services Manager
John Danielowich, Client Services Manager
Leigh Gagin, Client Services Manager
Sherri Klein, Client Services Manager

INFORMATION SYSTEMS
W. Michael Draper, Chief Operating Officer
Tom Kroon, Director of Systems Development
Anne Nickinello, Senior Systems Analyst
Puneet Narang, Manager of Database Technologies
William Zhang, Senior Software Engineer
Manav Sehgal, Senior Software Engineer
Jason Croci, Web Application Developer
Prashanth Menon, Database Support Specialist
Rocco Bortone, Director of Network IT
Peter Hebenstreit, Senior Network/Telecom Engineer
Brian Wood, Senior Systems Support Specialist
David Mahoney, Systems Support Specialist

BUSINESS SERVICES
Mark Anderson, Business Services Supervisor
Linda Cavanagh, Business Services Administrator

IDG

Patrick J. McGovern, Chairman of the Board
Bob Carrigan, President, IDG Communications

Network World is a publication of IDG, the world's largest publisher of computer-related information and the leading global provider of information services on information technology. IDG publishes over 300 computer publications in 85 countries. One hundred million people read one or more IDG publications each month. *Network World* contributes to the IDG News Service, offering the latest on domestic and international computer news.

Sales Offices

New York/New Jersey
Tom Davis, Associate Publisher, Eastern Region
Elisa Della Rocco, Regional Account Director
Agata Joseph, Sr. Account Coordinator
Internet: tdavis, elisas, ajoseph@nww.com
(201) 634-2300/FAX: (201) 634-9286

Northeast
Elisa Della Rocco, Regional Account Director
Internet: elisas@nww.com
(508) 460-3333/FAX: (508) 460-1237

Mid-Atlantic
Jacqui DiBianca, Regional Account Director
Internet: jdibian@nww.com
(610) 971-1530/FAX: (610) 975-0837

Midwest/Central
Tom Davis, Associate Publisher, Eastern Region
Agata Joseph, Sr. Account Coordinator
Internet: tdavis, ajoseph@nww.com
(201) 634-2314/FAX: (201) 712-9786

Southeast
Don Seay, Regional Account Director
Internet: dseay@nww.com
(404) 504-6225/FAX: (404) 504-6212

Northern California/Northwest
Sandra Kupiec, Associate Publisher, Western Region
Karen Wilde, Regional Account Director
Vanessa Tormey, Regional Account Director
Jennell Hicks, Regional Account Director
Jennifer Hallett, Account Coordinator
Cyril Talusan, Account Coordinator
Internet: skupiec, kwilde, vtormey, jhicks, ctalusan, jhallett@nww.com
(510) 768-2800/FAX: (510) 768-2801

Southwest/Rockies
Becky Bogart, Regional Account Director
Internet: bbogart@nww.com
(949) 250-3006/FAX: (949) 833-2857

Online/Integrated Solutions
Kevin Normandeau, Exec. Vice President/General Mgr., Online
Susan Cardoza, Associate Publisher, Online
Stephanie Gutierrez, Online Account Manager
Debbie Lovell, Online Account Manager
Kate Zinn, Online Account Director
Denise Landry, Account Coordinator
Lisa Thompson, Account Coordinator
Internet: knormandeau, scardoza, sgutierrez, dlovell, kzinn, dlandry, lthompson@nww.com
(508) 460-3333/FAX: (508) 861-0467

MARKETPLACE/EMERGING MARKETS
Donna Pomponi, Director of Emerging Markets
Enku Gubaie, Manager of Marketplace/Emerging Markets
Ceitlin Horgan, Maneger of Marketplace/Emerging Markets
Chris Gibney, Sales Operations Coordinator
Internet: dpomponi, egubaie, chorgan, cgibney@nww.com
(508) 460-3333/FAX: (508) 460-1192

Identity

continued from page 1

Identity and the network

A number of network access-control vendors slated to appear at this week's Digital ID World conference are adopting identity technology to help improve network and data security by integrating the network layer and the application layer.

Vendor	Product	Comment
Apere	Identity Managed Access Gateway	Combines provisioning tools with access control.
Applied Identity	Identiforce	Identity-based network access management.
Caymas	Identity-Driven Access Gateway	Network access control and SSL VPN in one box.
ConSentry Networks	LANShield Controller	Enforcement of user-based access controls.
Identity Engines	Ignition	Designed to replace RADIUS servers.
Trusted Network Technologies	Identity Driver; I-Manager; I-Gateway	Trio of products marries user data and policies.

develop their own NAC frameworks while providing methods for users to integrate the two.

They said interoperability would hinge in part on a single agent that will ship with Vista and Longhorn Server, and that will work on the Cisco and Microsoft platforms and can be used by third parties to tie their systems into the architecture. Cisco will continue to develop its Trust Agent to support non-Microsoft platforms.

The companies plan to begin a beta test with a limited number of users by year-end, but the entire architecture won't be available until Microsoft's Longhorn Server ships in late 2007.

By contrast, Caymas, ConSentry, TNT and others are shipping hardware and software that goes beyond validating that a machine is current on patches and antivirus and spyware signatures — which are the pre-admission to the network checks Cisco and MS initially are focused on — into postadmission controls that use identity and policies stored at the application layer to govern how the network looks and reacts to a particular user.

Users already are tallying up the benefits from tightened security, from compliance and auditing to easier management.

"From a security and services perspective, identity has been incredibly useful because we have had this perception that access was based on who you knew, and now we can articulate clearly what people get," says Jeremy Hobbs, CIO of the Upper Canada District School Board in Ontario. "From a manageability perspective, it has been enormous. Also, our auditors love it. They ask how do we decide who gets access to our financial system, and based on identity, we can say these job codes have access and everybody else doesn't."

During the past year, Hobbs has re-architected his network infrastructure so it controls access to resources via user identity and a set of rules, roles and policies, for example, a student's grade level; whether a user is a teacher or administrator; and a user's accumulated threat history.

Internally, the district has built its identity and access control on Microsoft's Active Directory and NAC tools from Nevis Networks. On the perimeter, it uses Caymas' Identity-Driven Access Gateway, integrated with permissions the district wrote and stores in Active Directory to control access for remote users.

"With Caymas, we can track people right down to individual files," Hobbs says.

The driving force is identity, and network vendors are seeing the light from many angles.

Caymas started off doing VPN termination, and ConSentry was a traditional NAC vendor. TNT started as an identity vendor and ended up in the network layer, where it puts identity information into packets.

Much of this identity-enabled hardware sits inline without requiring infrastructure overhauls, and works at wire speeds, so network architects don't introduce latency.

When a user's identity is added to a new group or job title, access control is based on that new identity and controls based on the old identity disappear automatically.

"All of our access control is based on the identity of users and machines," says Rob Ciampa, vice president of marketing and business strategy for TNT. "We set up access control rules on the back end so you don't have to configure access based on IP address and TCP or [User Datagram Protocol] ports."

TNT has helped the state of Georgia lock down its voter registration system, which serves 163 counties.

"I was mainly looking for some control over what machines could come into our network," says Wes Peters, a network engineer for the state.

Blocking machines by IP address via the firewall was not an option, Peters says, because many users did not have static IP addresses. Now he controls access to the network via the identity of specific trusted machines that have the TNT driver, and hides his Web site from hackers by limiting access to the logon screen to those trusted machines.

Others say that identity-enabled controls mean users no longer have to manage access-control lists, virtual LANs or firewall rules.

"By a user simply coming onto the network and authenticating, you can have the roles and responsibilities for that user enforced in the network based on policies that are stored in our engine or in RADIUS or Active Directory or [a Lightweight Directory Access Protocol] server," says Jeff Prince, CTO of ConSentry, which makes an appliance that sits behind the switching infrastructure.

The company plans to introduce this year its own Layer 2-3 10/100/1000Mbps switch that incorporates an identity-enabled appliance that will integrate with the NAP technology coming out with Microsoft's Vista desktop operating system.

Experts say they don't expect the network-layer identity trend to reach critical mass for another two to three years.

"We sort of feel that the identity piece is what is tying together a lot of preexisting security technologies," says Rob Ayoub, a network security analyst for Frost & Sullivan. "Identity is delivering on the promises of security that have been hinted at in the past but have not been fully realized." ■

ISS jumps into e-mail security fray

BY CARA GARRETSON

Security vendor Internet Security Systems this week plans to announce its foray into the packed e-mail security market with an appliance that does double duty: blocking spam and viruses while also preventing intrusion.

The Proventia Network Mail Security System will be available this month. It's designed to sit at an enterprise's gateway to block malicious e-mails from coming in and keep sensitive information from getting out, says Dave Ostrouski, senior manager of product marketing at ISS.

Despite the unique twist of adding IPS to spam and virus protection, ISS enters the e-mail security arena at a time when the overcrowded market is starting to mature and shake out, and companies have likely already placed their bets on the vendors they believe will survive.

ISS will go up against appliance makers Barracuda, CipherTrust, IronPort, Mirapoint, Proofpoint and others. The company asserts that because it offers products in other security areas — unlike many of its new competitors — organizations will want to standardize on ISS.

The Proventia Network Mail appliance blocks spam, viruses, worms, phishing attacks and other malicious code attempting to enter an organization through the inbound mail stream. It includes ISS' existing Virus Prevention System, which examines the behavior of network traffic to detect viruses before signature matches are released for them, Ostrouski says. The company also offers Sophos' antivirus technology as an add-on module.

Proventia Network Mail applies keyword matching to outbound e-mail messages so companies can ensure employees aren't sending out information protected by regulation or corporate policy, Ostrouski says.

The Proventia Network Mail Security System appliance, with integrated IPS, costs $20,300 and can support as many as 2,500 users. ■

■ **Network World**, 118 Turnpike Road, Southborough, MA 01772-9108, (508) 460-3333.

Periodicals postage paid at Southborough, Mass., and additional mailing offices. Posted under Canadian International Publication agreement #40063800. Network World (ISSN 0887-7661) is published weekly, except for a single combined issue for the last week in December and the first week in January by Network World, Inc., 118 Turnpike Road, Southborough, MA 01772-9108.

Network World is distributed free of charge in the U.S. to qualified management or professionals.

To apply for a free subscription, go to www.subscribenw.com or write Network World at the address below. No subscriptions accepted without complete identification of subscriber's name, job function, company or organization. Based on the information supplied, the publisher reserves the right to reject non-qualified requests. Subscriptions: 1-508-490-6444.

Nonqualified subscribers: $5.00 a copy; U.S. - $129 a year; Canada - $160.50 (including 7% GST, GST#126659952); Central & South America - $150 a year (surface mail); all other countries - $300 a year (airmail service). Four weeks notice is required for change of address. Allow six weeks for new subscription service to begin. Please include mailing label from front cover of the publication.

Network World can be purchased on 35mm microfilm through University Microfilm Int., Periodical Entry Dept., 300 Zeeb Road, Ann Arbor, Mich. 48106.

POSTMASTER: Send Change of Address to **Network World**, P.O. Box 3090, Northbrook, IL 60065. Canadian Postmaster: Please return undeliverable copy to PO Box 1632, Windsor, Ontario N9A7C9.

USPS735-730

Oath

continued from page 1

thing he doesn't miss is the raids. "I got a little tired of running up flights of stairs, breaking in doors," says Megerian, who retired from the Treasury Department in 2003 after 29 years.

In his consulting practice Megerian works primarily with government clients, investigating financial fraud and other criminal activities. He's among a growing number of computer forensics specialists trained to pore through hard drives and device logs to find evidence of criminal or inappropriate behavior.

As digital evidence has become more important to civil and criminal cases, the field has gained recognition, says Alan Brill, senior managing director at Kroll Ontrack, in Minneapolis. Interest in computer forensics also has grown because of the state-of-the-art labs and slick extractions of digital evidence viewers see portrayed on television shows such as "CSI."

"It is not what it looks like on TV," Brill says. "When we watch some of these shows where the cops go in and they sit at a suspect's computer and they find all this evidence — it's not what happens."

Rather, computer forensics is all about protocol. Experts use established investigative and analysis techniques to uncover system data — including damaged, deleted, hidden or encrypted files.

"People think that it's glamorous. The reality is that 95% of the time it's about very routine analytics and executing projects in a very uniform way," Brill says. "It is certainly not for those who are not detail- and process-oriented. It is not for those who loathe documenting their work, because the nature of what we do requires very complete, careful documentation."

As projects unfold, the digital evidence accumulates. In one case Brill worked on, a company suspected an individual of sabotaging computer systems. It was clear from which machine the sabotage occurred, but to prove who was responsible took some digging.

"The bad guy claimed he couldn't have done it, he was outside smoking a cigarette," Brill recalls. Video from the building security system appeared to confirm that alibi, with a time stamp indicating he was there when the sabotage happened, Brill says.

After examining additional sources, however, Brill and his team found the time clock in the video system was inaccurate. They dug into the building's access-control system — which has a time clock of its own — and determined when the suspect used his badge to return to his office after a smoking break.

A check of phone logs supplied further evidence suggesting the suspect's culpability. "At the time of the incident, somebody was using the telephone on that very desk. And that somebody turned out to be telephoning the unlisted number of our suspect's mother," Brill says.

Spoliation happens

As important as what gets found is how it's found. "When you analyze a computer you're doing several things. The most important is preservation of evidence," Megerian says. If data isn't extracted properly — whether it's contained in router logs, hard drives, e-mail servers or any other electronic storage media — it can't be produced for evidence, he says.

"Getting data in a way that would be admissible in a court is different than just grabbing things. We run into cases all the time where the IT staff wants to capture data for their company but ends up making mistakes that render the data either questionable or inadmissible," Brill says. "There is a term for damaging or destroying evidence, whether it's done intentionally or not. It's called spoliation."

IT isn't the only culprit. Corporate investigators, internal auditors and legal staff have spoiled a crime scene inadvertently while snooping for information. "It's a very natural impulse. The only problem is that if you're looking at things forensically, there's a protocol you have to follow," Brill says. People dabbling with forensic evidence don't always recognize the limitations of their knowledge, he says.

Something as simple as printing a file can be damaging, because the creation of temporary files during the printing process can overwrite potentially significant content. "What was the content of the storage areas onto which those temporary files were written? We're never going to know because they covered it up with new data," Brill says.

Those in the trade use specialized tools such as write-blockers, which are designed to make an image of a hard drive without disturbing its contents. "It's a piece of specialized hardware that prevents us from sending any signal to the hard drive that would cause it to write any characters," Brill explains.

"We capture literally everything. If it's an 80GB drive, we capture 80GB of data whether there are files there or not. We have to capture every byte — because evidence may be in what a user might think of as empty space — and we have to do it in a way that we can document and testify to," Brill says.

For IT, there's an opportunity to play a pivotal, first-responder type of role in the early stages of a criminal or civil investigation. Having an IT staff member trained in computer forensics is a good way to protect potential legal evidence from being destroyed, Megerian says.

"IT people are the first ones on the scene when something goes wrong with the network, if a company is attacked or a rogue employee does something illegal," he says. One or two members of the IT staff should be trained to handle the situation without damaging evidence, while protecting the chain of custody of the evidence, he says.

"If a network goes down you need to get the network back up and running. But there's still time to do it in such a manner that you preserve the evidence," Megerian says. "It's like an accident scene or a robbery scene. Put that yellow caution tape all around and don't let anybody in."

Taking an oath

Procuring admissible evidence is critical, because discovery is just the beginning of the process. Computer forensics specialists turn over their findings to clients — criminal prosecutors, civil litigators, insurance companies and corporations that are investigating crimes (homicides, financial fraud and child pornography, for example) and civil matters (such as divorce, intellectual property theft and harassment).

Forensics experts may be asked to explain their findings via a deposition or court appearance. By most accounts, avoiding a court appearance is a good thing.

Testifying in court isn't a pleasant experience, because the opposing side will do what it can to discredit an evidence witness, Megerian says. "You're going to be going up against experts that the other side will put on. You have to be able to withstand the rigors in court," he says.

"It's pretty hairy," agrees Stuart Hanley, senior electronic evidence consultant at Kroll Ontrack. "The attorneys are not going to be nice. They are going to be as nasty as they can. They'll ask the same questions six different ways, trying to trip you up or get you to say something that's a little bit more in their favor."

A memorable court appearance for Hanley took place in 2000, when he was answering to a team of White House attorneys. His testimony involved technical issues related to the copying, restoration and retrieval of e-mail from the Clinton-Gore administration. When the attorneys couldn't find holes in his testimony, they asked more personal questions: Which candidate had Hanley voted for in the last presidential election? Had he been compensated for his trip to Washington, D.C.? "That was some very rowdy, stressful testifying," he recalls.

Fortunately it's rare that a court testimony is required, Brill says. "More often than being on the stand, we have to give depositions," he says. "In essence, you're testifying. Not in court, but to a court reporter and often a videographer. You're under oath, and that record is admissible."

Withstanding legal scrutiny isn't the only hard part of the job. An ongoing challenge is keeping up with hardware and software advances that can affect a forensic analysis. And it gets harder as bad guys get more industrious about obscuring their digital tracks. "In computer forensics, every day you realize how much you don't know. I've never seen anything like it," Megerian says. "Trying to stay on top of it probably involves 50% of my time."

It's also not a job for homebodies. Although some work is done in a lab setting, there's also plenty of time spent in the field extracting and analyzing evidence. ■

Learning to be a first responder

Computer forensics training is available from universities and professional organizations around the world. Here are a few U.S. sources.

Provider	Offering	Location	URL
George Mason University	Computer forensics training.	Online course	http://ocpe.gmu.edu/certificate_programs/online/forensic_computer.html
George Washington University	Master's degree in forensic science with a concentration in high-tech crime investigation.	Arlington, Va.	www.gwu.edu/%7Eforensic/htci.htm#Top_page
Eastern Michigan University, Center for Regional and National Security	Computer forensics training.	Ypsilanti, Mich.	www.emich.edu/cerns/ec/ec_forensic_overview.htm
InfoSec Institute	Computer forensics training.	Chicago and around the United States	www.infosecinstitute.com/courses/computer_forensics_training.html
Kennesaw State University	Continuing education program in computer forensics.	Kennesaw, Ga.	www.kennesaw.edu/coned/sci/index.htm
University of Central Florida	Graduate certificate in computer forensics.	Orlando	www.cs.ucf.edu/csdept/info/gccf/

Take back control with an IBM I.T. Optimization Solution.

***Control your resources** with IBM Systems and Middleware, which let you virtualize and simplify your I.T. and manage your applications and systems from a single point of control.*

***Control your costs** and improve utilization of your existing I.T. resources by consolidating and simplifying your servers, storage, apps and network assets.*

***Control your efficiency** by automating manual tasks to reduce errors, manage availability and dynamically allocate I.T. resources as needed.*

***Control your I.T. destiny** with IBM Systems, Middleware and Services – a proven set of solutions designed to take your company from reactive to proactive.*

Try the Infrastructure Benchmark Assessment Tool at:
IBM.COM/**TAKEBACKCONTROL**/OPTIMIZE

BACKSPIN Mark Gibbs

The rules of IT

Wherever you go and whatever you do, it is a given that some set of rules will be in force. Rules matter because they define how we get on with other people and what is considered normal.

If you want to drive, you need to know the rules of the road, and if you want to be socially acceptable, you need to know the rules of behavior for eating in public and attending parties. The list is endless, and we learn many simply by growing up in a culture.

You can see from those examples that while some rules are written down and clearly laid out — for example, rules for games, writing, flying aircraft and sailing boats — there are thousands of rules that are not codified.

These informal rules are learned from experience or because someone was kind enough to lay them out for you. These are rules of convention that countless years have evolved to regulate society, protect individuals and keep us from throwing away a million years of evolution and resorting to hitting each other with rocks.

Which brings me to the rules of IT. There are a number you must observe if you plan to have a career in IT:

Rule No. 1: Do not annoy the guys with money. That means everyone above you with any influence on your budget or salary. They are all your best friends or, at worst, close acquaintances no matter how annoying and loathsome they may be.

Rule No. 2: Always back up first. No matter how simple the task, if you change something, and you haven't got a backup in the bag, you are flirting with disaster. This rule is covered by Murphy's Law: If something can go wrong, it will. And without a backup, it will. Particularly changing router tables.

Rule No. 3: The leading edge isn't. No matter what you are told by the press, the vendors, the resellers, the integrators or anybody, the leading edge should be nowhere near your shop unless you have insanely huge piles of money and can avoid taking responsibility for cosmic-level disasters.

Rule No. 4: Document everything. You never know when that off-the-cuff, seemingly harmless request from a CXO is going to turn out to be a huge python that wraps itself around your throat. If he (or anyone else) asks for anything that has even vaguely related IT repercussions, then get it in writing. Going to change the router tables? Back up first (see Rule No. 2) and then document what you did and why. When I say document everything, I mean everything. In some organizations this might even include bathroom breaks.

Rule No. 5: Document nothing (see Rule No. 4). Once you document everything and make it known that you do so, you should then make sure nothing that implicates you as to being part of the decision process gets documented. Plausible deniability is what we're looking for.

Rule No 6: It is not your fault. Whatever it is, someone else is responsible. And you have the paperwork to prove it (see rule Nos. 4 and 5).

Rule No. 7: Do unto users before they do unto you. There's a fine balance between career-furthering, fawning care and feeding of users and the satisfying but inadvisable practice of torturing them. Get the balance right, and you will be seen as fair but firm. Get it wrong, and you are a bastard who needs to update his résumé.

Rule No. 8: You can't afford any piece of equipment or software that is priced high enough to make you shudder. If you have to have it, then it must not be your decision (no matter how much influence you think you have), and your signature won't be on the purchase order, will it?

Rule No. 9: Always tell the truth, never tell a lie and never be the one to change the router tables (see rule Nos. 2, 4 and 6).

Rule No. 10: Always cover your arse (see Rule Nos. 1, 2, 4, 5, 6 and 8).

Tell backspin@gibbs.com your rules or comment on Gibbsblog.

Adam Gaffin

COMPENDIUM

CompUSA's online ordering could use help

In theory, CompUSA's online ordering and pickup system is pretty cool: You find the item you want, see which nearby stores have it and submit a reservation so it is waiting for you when you get to the store (CompUSA promises it will be ready within 15 minutes of your reserving it).

For me, anyway, this all remains strictly theoretical. A few months ago, I reserved a digital camera. When I got to the store, the camera was nowhere around, and somebody had to go find it. (This was about 40 minutes later.)

But that was nothing compared with my experience a few days ago when I needed a new power adapter for a laptop. I went to the CompUSA Web site, found the model I needed and reserved it at a CompUSA about 20 minutes from home.

My daughter and I drove over. I stood in the customer service line for about 10 minutes then finally got to the desk and gave the representative my pickup number. She rummaged around out back for a while but couldn't find the adapter. She paged the manager, who searched for it. Some 20 minutes later the manager was still looking around. I passed the time at this pedestal-mounted, Internet-connected PC that CompUSA has thoughtfully provided, complaining about this on my nonwork blog.

The manager finally showed up about five minutes after that. Adapter in hand? No — he explained that the online ordering system is not updated in real time, and so it lets you order things the store does not actually have in stock (one saving grace: They did have another adapter that would work). Next time, I think I'll try another chain.

Letting people use your Web service

So you've got this spiffy new way to access some data set. And you want to let other people mash it up and do cool stuff with it. Of course you'll need an API. Ryan Campbell, a database specialist for Wufoo, has written a how-to, with PHP examples.

www.nwdocfinder.com/5157

Google tells some people to turn off their firewalls

Martin McKeay writes on his network security blog that Google's answer to people trying to read particular kinds of e-mail is to tell them to turn off their firewalls. He is not amused: "Even if the firewall service restarts next time the user starts up his or her computer, that still might mean they're without protection for hours, possibly days."

www.nwdocfinder.com/5158

What goes better with free software than free beer?

Free as in no licensing requirements, that is. A group of Danish artists and students are trying to adapt open source licensing (specifically, a Creative Commons copyright) to the art of beer making:

"The recipe and branding elements of FREE BEER is published under a Creative Commons (Attribution-ShareAlike 2.5) license, which means that anyone can use the recipe to brew their own FREE BEER or create a derivative of the recipe. Anyone is free to earn money from FREE BEER, but they must publish the recipe under the same license and credit our work. All design and branding elements are available to beer brewers, and can be modified to suit, provided changes are published under the same license (Attribution & Share Alike)."

www.nwdocfinder.com/5159

What would Jesus run?

Ubuntu Christian Edition is a Linux distribution that comes bundled with a Bible, a Bible study unit and a parental-control module to keep impressionable young'uns away from temptation: "These features are truly what sets Ubuntu Christian Edition apart."

www.nwdocfinder.com/5160

Paul McNamara returns next week. Get more Compendium at www.nwdocfinder.com/5162.

How the Doughboy graces millions of dinner tables. Always in a timely fashion.

Each day, Pillsbury products and other General Mills brands appear in millions of shopping carts around the world. HP Integrity servers with Intel® Itanium® 2 processors help keep distribution and inventory control systems running smoothly. "With their continuous performance and support, we are able to ensure that customer orders and shipments are processed quickly and accurately," said Vandy Johnson, Director of I.S. Operations. "And that's a comforting thought." itanium-integrity.com

ITANIUM + INTEGRITY. ON AND ON AND ON.